Anwenderhandbuch

TAINY HMOD-V2-IO, TAINY HMOD-L1-IO
TAINY EMOD-V2-IO, TAINY EMOD-L1-IO

Dr. Neuhaus

Copyright Statement

Die in dieser Publikation veröffentlichen Beiträge sind urheberrechtlich geschützt. Übersetzungen, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen bedürfen der ausdrücklichen Genehmigung der Dr. Neuhaus Telekommunikation GmbH.

© 2012 Dr. Neuhaus Telekommunikation GmbH

Alle Rechte vorbehalten.

Dr. Neuhaus Telekommunikation GmbH

Papenreye 65, D-22453 Hamburg

Fax.: +49 (40) 55304-180

Internet: http://www.neuhaus.de

E-Mail: Kundendienst@neuhaus.de

Technische Änderungen vorbehalten.

TAINY® ist ein Warenzeichen der Dr. Neuhaus Telekommunikation GmbH. Alle anderen Warenzeichen und Produktbezeichnungen sind Warenzeichen, eingetragene Warenzeichen oder Produktbezeichnungen der jeweiligen Inhaber.

Alle Lieferungen und Leistungen erbringt die Dr. Neuhaus Telekommunikation GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der Dr. Neuhaus Telekommunikation GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Produkt-Nr.: 3173, 3183

Dok.-Nr.: 3183AD001 Version 2.1

Produkte: TAINY HMOD-V2-IO, TAINY EMOD-V2-IO

TAINY HMOD-L1-IO, TAINY EMOD-L1-IO

Ab Firmware-Version 1.309

Sicherheitshinweise

Produkte

Die Bezeichnung TAINY xMOD wird im Folgenden als Sammelbegriff für das TAINY HMOD-V2-IO, TAINY HMOD-L1-IO, TAINY EMOD-V2-IO, TAINY EMOD-L1-IO verwendet.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems dürfen nur von qualifiziertem Personal vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Allgemeine Hinweise zu dem Produkt

Das Produkt TAINY xMOD entspricht der europäischen Norm EN60950 (11.2006), Einrichtungen der Informationstechnik - Sicherheit. Lesen Sie vor Gebrauch des Gerätes die Installationsanleitung sorgfältig durch. Halten Sie das Gerät von Kindern fern, besonders von Kleinkindern. Das Gerät darf nicht im Freien oder in Feuchträumen installiert und betrieben werden. Nehmen Sie das Gerät nicht in Betrieb, wenn Anschlussleitungen oder das Gerät selbst beschädigt sind.

Externe Stromversorgung

Verwenden Sie nur eine externe Stromversorgung die ebenfalls der EN60950 entspricht. Die Ausgangsspannung der externen Stromversorgung darf 60V DC nicht überschreiten. Der Ausgang der externen Stromversorgung muss kurzschlussfest sein.

Das TAINY xMOD darf nur aus Stromversorgungen nach IEC/EN60950 Abschnitt 2.5 "Stromquelle mit begrenzter Leistung" versorgt werden. Die externe Stromversorgung für das TAINY xMOD muss den Bestimmungen für NEC Klasse 2 Stromkreisen entsprechen, wie im National Electrical Code ® (ANSI/NFPA 70) festgelegt.

Bei Anschluss an eine Batterie oder einen Akkumulator beachten Sie, dass zwischen dem Gerät und der Batterie oder Akkumulator eine allpolige Trennvorrichtung (Batteriehauptschalter) mit ausreichendem Trennvermögen sowie eine Sicherung mit ausreichendem Trennvermögen vorzusehen sind (z. B. Pudenz FKS Sicherungssatz 32 V, 3 A, Best.-Nr. 162.6185.430).

Beachten Sie den Abschnitt Technische Daten dieser Dokumentation (Kapitel 13) sowie die Einbau- und Nutzungsvorschriften des jeweiligen Herstellers der Stromversorgung, der Batterie oder des Akkumulators.

Schalteingang und Schaltausgang

Der Schalteingang und der Schaltausgang sind jeweils gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schalteingangs oder des Schaltausgangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schalteingangs oder des Schaltausgangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

Umgang mit Kabeln

Ziehen Sie niemals einen Kabelstecker am Kabel aus seiner Buchse, sondern ziehen Sie am Stecker. Führen Sie die Kabel nicht ohne Kantenschutz über scharfe Ecken und Kanten. Sorgen Sie gegebenenfalls für eine ausreichende Zugentlastung der Kabel. Achten Sie bitte darauf, dass aus Sicherheitsgründen der Biegeradius der Kabel eingehalten wird. Die Nichteinhaltung der Biegeradien des Antennenkabels führt zu Verschlechterung der Sende- und Empfangseigenschaften des Gerätes. Der minimale Biegeradius darf statisch den 5-fachen Kabeldurchmesser und dynamisch den 15-fachen Kabeldurchmesser nicht unterschreiten.

Funkgerät

Verwenden Sie das Gerät niemals in Bereichen, in denen der Betrieb von Funkeinrichtungen untersagt ist. Das Gerät enthält einen Funksender, der gegebenenfalls medizinische elektronische Geräte wie Hörgeräte oder Herzschrittmacher in ihrer Funktion beeinträchtigen kann. Ihr Arzt oder der Hersteller solcher Geräte können Sie beraten. Damit keine Datenträger entmagnetisiert werden, lagern Sie bitte keine Disketten, Kreditkarten oder andere magnetische Datenträger in der Nähe des Gerätes.

Antennen-Montage

Das Einhalten der empfohlenen Strahlungsgrenzwerte der Strahlenschutzkommission vom 13./14. September 2001 muss gewährleistet sein.

Montage einer Außenantenne

Bei der Installation einer Antenne im Freien ist es zwingend erforderlich, dass die Antenne durch Fachpersonal fachgerecht montiert wird. Die Einhaltung der Blitzschutznorm VDE V 0185 Teil 1 bis 4 in ihrer aktuellen Fassung und weiterführende Normen sind dabei vorgeschrieben.

Die Gebäude-Blitzschutzklasse (SK)

Bei der Außenmontage darf die Antenne nur innerhalb der Blitzschutzzonen O/E bzw. 1 angebracht werden. Diese Blitzschutzzonen werden durch den Blitzschutzkugelradius vorgegeben.

Das EMV Blitzschutzzonen-Konzept

Das EMV Blitzschutzzonen-Konzept ist einzuhalten. Um große Induktionsschleifen zu vermeiden, ist ein Blitzschutz-Potentialausgleich anzuwenden. Werden Antenne oder Antennenkabel in der Nähe der Blitzschutzanlage montiert, müssen die Mindestabstände zur Blitzschutzanlage eingehalten werden. Ist dies nicht möglich, ist eine isolierte Montage wie in der Blitzschutznorm VDE V 0185 Teil 1 bis 4, in ihrer aktuellen Fassung beschrieben, zwingend erforderlich.

Hinweise zu FCC Part 15

FCC Part 15

Aufgrund entsprechender Tests wurde befunden, dass dieses Gerät den Grenzwerten für digitale Geräte der Klasse A entspricht, gemäß der FCC Rules Part 15. Diese Grenzwerte sind so festgelegt, dass bei ihrer Einhaltung angemessener Schutz gegen schädliche und störende Interferenzen gewährleistet ist, wenn das betreffende Gerät im Wohnbereich installiert ist. Dieses Gerät erzeugt und benutzt Hochfrequenzen und kann diese ausstrahlen. Wenn dieses Gerät nicht in Übereinstimmung mit den Instruktionen installiert und benutzt wird, kann es störende Interferenzen für den Funkverkehr bewirken. Es kann jedoch nicht garantiert werden, dass es bei bestimmten Installationen, auch wenn diese in Übereinstimmung mit den Instruktionen vorgenommen werden, keine störenden Interferenzen geben kann. Falls dieses Gerät störende Interferenzen beim Radio- oder Fernsehempfang bewirkt, was durch Ein- und Ausschalten des Gerätes ermittelt werden kann, empfehlen wir dem Benutzer, folgende Gegenmaßnahmen zu ergreifen.

- Ändern Sie die Ausrichtung der Empfangsantenne oder installieren Sie diese an anderer Stelle.
- Vergrößern Sie den Abstand zwischen dem TAINY xMOD und dem Radio- oder Fernsehempfänger.
- Schließen Sie das Gerät an eine Netzsteckdose an, die sich in einem anderen Stromkreis befindet als die, an der der Empfänger angeschlossen ist.
- Wenden Sie sich an einen Fachhändler / Installateur oder an einen kompetenten Fachmann für TV und Radioempfang und fragen Sie ihn.

FCC Part 15.19

Dieses Gerät entspricht den Bestimmungen in Part 15 der FCC Rules. Sein Betrieb unterliegt folgenden Bedingungen:

1. Dieses Gerät bewirkt möglicherweise keine schädlichen oder störenden Interferenzen, und
2. Dieses Gerät muss empfangene Interferenzen hinnehmen können, auch solche, die ein unerwünschtes Betriebsverhalten bewirken könnten.

FCC Part 15.21

Modifikationen am Gerät, denen dieser Hersteller nicht ausdrücklich zugestimmt hat, können dazu führen, dass der Benutzer nicht mehr befugt ist das Gerät zu betreiben.

Installation nur durch Fachpersonal

Das TAINY xMOD darf nur mit einer Antenne aus dem Zubehörsortiment des TAINY xMOD betrieben werden.

Ausschließlich Fachpersonal darf das TAINY xMOD und dessen Antenne installieren und warten. Bei Arbeiten an der Antenne oder bei Arbeiten näher als unten angegeben muss der Sender ausgeschaltet sein.

HF-Exposition

Normalerweise arbeitet die am Sender dieses Gerätes angeschlossene Antenne in allen Richtungen mit 0 dB Verstärkung. Die Composite Power im PCS-Modus ist bei Benutzung dieser Antenne geringer als 1 Watt ERP.

Die mit diesem mobilen Gerät benutzen internen / externen Antennen müssen mindestens 20 cm von Personen entfernt sein. Und sie dürfen nicht so platziert oder betrieben werden, dass sie in Verbund mit einer anderen Antenne oder Sender arbeiten.

Funkstörungen

Das TAINY xMOD ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Vorsicht Kosten

Bitte beachten Sie, dass auch beim (Wieder-) Aufbau einer Verbindung, bei Verbindungsversuchen zur Gegenstelle (z.B. Server ausgeschaltet, falsche Zieladresse, etc.) sowie zum Erhalt einer Verbindung kostenpflichtige Datenpakete ausgetauscht werden. So kann zum Beispiel eine nicht erreichbare Gegenstelle dazu führen, dass duch mißlungene Versuche beim Verbindungsaufbau zusätzliche Kosten entstehen.

Firmware mit Open Source GPL/LGPL

Die Firmware von TAINY xMOD enthält open Source Software unter GPL/LGPL Bedingungen. Gemäß des Abschnitts 3b von GPL und des Abschnitts 6b von LGPL bieten wir Ihnen den Quellkode an. Sie finden den Quellkode auf unserer Web-Seite im Internet www.neuhaus.de.

Alternativ können Sie den Quellkode auch bei uns auf CD-ROM anfordern. Senden Sie eine eMail an Kundendienst@neuhaus.de. Als Betrifftext Ihrer E-Mail geben Sie bitte 'Open Source xMOD' an, um Ihre Nachricht leicht herausfiltern zu können.

Die Lizenzbedingungen der open Source Software erhalten Sie mit dem Quellkode.

Firmware mit OpenBSD

Die Firmware von TAINY xMOD-V2-IO enthält Teile aus der OpenBSD-Software. Die Verwendung von OpenBSD-Software verpflichtet zum Abdruck des folgenden Copyright-Vermerkes:

```
* Copyright (c) 1982, 1986, 1990, 1991, 1993
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    This product includes software developed by the University of
*    California, Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

Ein Wort von unserem Technischen Kundendienst

Wir, die Techniker des Kundendienstes der Dr. Neuhaus Telekommunikation GmbH, begrüßen Sie recht herzlich. Sollten Sie bei der Inbetriebnahme Ihres neuen Geräts Schwierigkeiten haben, sind wir Ihre Ansprechpartner, und wir helfen Ihnen gern. Auch bei speziellen und ungewöhnlichen Konstellationen in Hardware und Software werden Sie bei uns immer ein offenes Ohr finden, wenn einmal nicht alles sofort klappen will. Der gute Ruf unserer Produkte beruht auch darauf, dass unseren Kunden stets ein Team kundiger Fachleute zur Verfügung steht, das sich auch auf ungewöhnliche Konstellationen einlässt. Sie erreichen uns unter **Kundendienst@neuhaus.de**.

Umweltschutz ist auch unser Thema

Der Erhalt einer lebenswerten Umwelt, d.h. die sinnvolle Verknüpfung von Ökologie und Ökonomie, ist eine der wichtigsten Aufgaben unserer Zeit. Wir begegnen dieser Herausforderung durch:

Qualität

Bedarfsorientierte Entwicklung und Produktion, eingebettet in modernste Qualitätssicherungsmechanismen, sorgen für Erzeugnisse höchster Qualität und langer Nutzbarkeit.

Rücknahmegarantie

Wir sind stolz auf unsere Produkte. Doch geben wir gern zu, dass diese nicht ewig leben. Darum stellen wir, soweit technisch schon möglich und sinnvoll, alle unsere Produkte aus wieder verwendbaren Materialien her. Wir garantieren, dass wir jedes von uns gefertigte Gerät zurücknehmen, die wieder verwendbaren Teile dem Recycling zuführen und den Rest umweltfreundlich entsorgen. Dazu wenden Sie sich an unser Service-Zentrum

Dr. Neuhaus Telekommunikation GmbH
Service-Zentrum
Messestraße 20,
D-18069 Rostock

Bitte helfen Sie uns dabei, die Umwelt zu schützen.

Dr. Neuhaus Telekommunikation GmbH

Inhaltsverzeichnis

1 Einleitung 9
2 Inbetriebnahme 14
2.1 Schritt für Schritt 14
2.2 Voraussetzungen für den Betrieb 15
2.3 Überblick 16
2.4 Service-Taster 16
2.5 Betriebsanzeigen 17
2.6 Anschlüsse 20
2.7 Die SIM-Karte einlegen 22
3 Konfiguration 23
3.1 Übersicht 23
3.2 Erlaubte Zeichen bei Benutzernamen, Passwörtern und weiteren Eingaben 23
3.3 TCP/IP Konfiguration des Netzwerkadapters unter Windows XP 24
3.4 Konfigurations-Verbindung herstellen 25
3.5 System Status (Startseite) 28
3.6 Konfiguration vornehmen 30
3.7 Konfigurations-Profile 31
3.8 Passwort ändern 32
3.9 Neustart 33
3.10 Werkseinstellung laden 33
3.11 Geräteidentifikation 34
4 Lokale Schnittstelle 35
4.1 IP-Adressen der lokalen Schnittstelle 35
4.2 DHCP-Server zum lokalen Netz 35
4.3 DNS zum lokalen Netz 37
4.4 Lokaler Hostname 38
4.5 Systemzeit / NTP 38
4.6 Zusätzliche interne Routen 39
5 Externe Schnittstelle 41
5.1 Netzauswahl und Zugangsparameter für UMTS bzw. EGPRS und GPRS 41
5.2 Überwachung der Datenfunkdienst-Verbindung 45
5.3 Hostname durch DynDNS 46
5.4 Secure DynDNS 47
5.5 NAT – Network Address Translation 48
5.6 Installationsmodus 49
5.7 Volumenüberwachung 50
6 Sicherheitsfunktionen 52
6.1 Paketfilter 52
6.2 Port Weiterleitung 55

6.3 Erweiterte Sicherheitsfunktionen ... 56
6.4 Firewall-Logbuch ... 57
7 VPN-Verbindungen ... 58
7.1 Einleitung ... 58
7.2 VPN Roadwarrior-Modus ... 60
7.3 VPN IPsec Standard-Modus ... 64
7.4 VPN Zertifikate laden ... 71
7.5 Firewall-Regeln für VPN-Tunnel ... 72
7.6 Überwachung der VPN-Verbindungen ... 73
7.7 Erweiterte Einstellungen bei VPN-Verbindungen ... 75
7.8 Status der VPN-Verbindungen ... 76
8 Fernzugänge ... 77
8.1 Fernzugang HTTPS ... 77
8.2 Fernzugang – SSH ... 78
8.3 Fernzugang über Wählverbindung ... 80
9 Logbuch, Update und Diagnose ... 82
9.1 Anzeige Logbuch ... 82
9.2 Remote Logging ... 83
9.3 Snapshot ... 84
9.4 Hardware Informationen ... 85
9.5 Software Informationen ... 85
9.6 Software Update ... 86
10 SMS-Versand ... 87
10.1 Service Center ... 87
10.2 Alarm SMS ... 87
10.3 SMS-Versand aus dem lokalem Netzwerk ... 88
11 SNMP ... 91
11.1 Bedienung per SNMP ... 91
11.2 Alarmmeldungen per SNMP-Traps ... 93
12 Kleines Router-Lexikon ... 95
13 Technische Daten ... 110
13.1 TAINY HMOD-V2-IO, TAINY HMOD-L1-IO ... 110
13.2 TAINY EMOD-V2-IO, TAINY EMOD-L1-IO ... 112

1 Einleitung

Produkte

Dieses Handbuch gibt Anweisungen zur Sicherheit und beschreibt die Bedienung und Installation folgender Produkte:

	VPN Funktion	HSDPA / UMTS	E-GPRS	GPRS	CSD
TAINY HMOD-V2-IO	**X**	**X**	**X**	**X**	**X*)**
TAINY HMOD-L1-IO	**-**	**X**	**X**	**X**	**X*)**
TAINY EMOD-V2-IO	**X**	**-**	**X**	**X**	**X**
TAINY EMOD-L1-IO	**-**	**-**	**X**	**X**	**X**

*) Nur wenn nicht in einem HSDPA / UMTS Netz eingebucht

Verwendete Produktbezeichnungen

In diesem Handbuch werden Sammelbegriffe für die verschiedenen TAINY-Produktvarianten verwendet:

TAINY xMOD	Sammelbegriff für TAINY HMOD-V2-IO, TAINY HMOD-L1-IO, TAINY EMOD-V2-IO, TAINY EMOD-L1-IO.
TAINY HMOD	Sammelbegriff für TAINY HMOD-V2-IO und TAINY HMOD-L1-IO.
TAINY EMOD	Sammelbegriff für TAINY EMOD-V2-IO und TAINY EMOD-L1-IO.
TAINY xMOD-V2-IO	Sammelbegriff für das TAINY HMOD-V2-IO und TAINY EMOD-V2-IO.
TAINY xMOD-L1-IO	Sammelbegriff für das TAINY HMOD-L1-IO und TAINY EMOD-L1-IO.

Anwendung

Die TAINY xMOD bieten einen drahtlosen Anschluss zum Internet oder zu einem privaten Netzwerk.

Die TAINY HMOD bieten diesen Anschluss an jedem Ort, an dem ein UMTS-Netz (Universal Mobile Telecommunication System = Mobilfunknetz 3. Generation) oder ein GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das IP-basierte Datendienste bereitstellt. Bei UMTS sind dies der HSDPA Data Service (High Speed Download Data Access) oder der UMTS Data Service und bei GSM sind dies EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service).

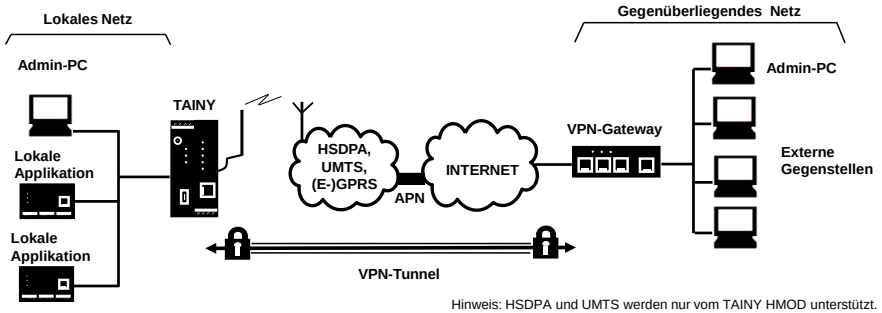
Die TAINY EMOD bieten diesen Anschluss an jedem Ort, an dem ein GSM-Netz (Global System for Mobile Communication = Mobilfunknetz) verfügbar ist, das als Dienste EGPRS (Enhanced General Packet Radio Service = EDGE) oder GPRS (General Packet Radio Service) bereitstellt. Voraussetzung dafür ist eine SIM-Karte eines Mobilfunkbetreibers mit entsprechend freigeschalteten Diensten.

Die TAINY xMOD-L1-IO verbinden so eine lokal angeschlossene Applikation oder ganze Netzwerke über drahtlose IP-Verbindungen mit dem Internet. Möglich ist auch die direkte Verbindung mit einem Intranet an dem wiederum die externen Gegenstellen angeschlossen sind.

Die TAINY xMOD-V2-IO können über eine drahtlose IP-Verbindung ein VPN (Virtual Private Network) zwischen einer lokal angeschlossene Applikation/ einem Netzwerk und einem externen Netz aufbauen und diese Verbindung mittels IPsec (Internet Protocol Security) gegen Zugriffe Dritter schützen.

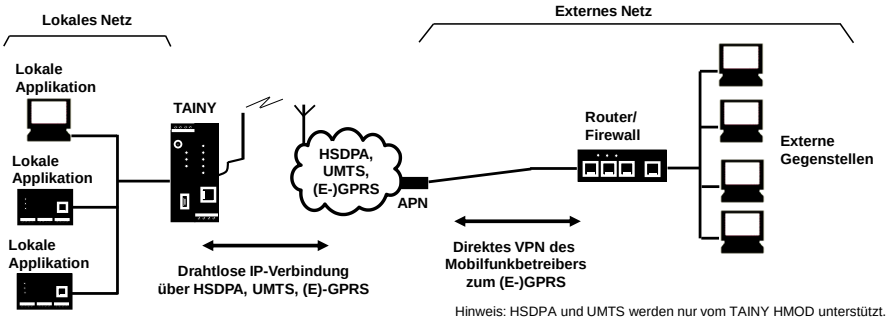
Szenarium 1: Virtual Private Network (VPN) mit Ipsec (Ende zu Ende)

Nur TAINY xMOD-V2-IO



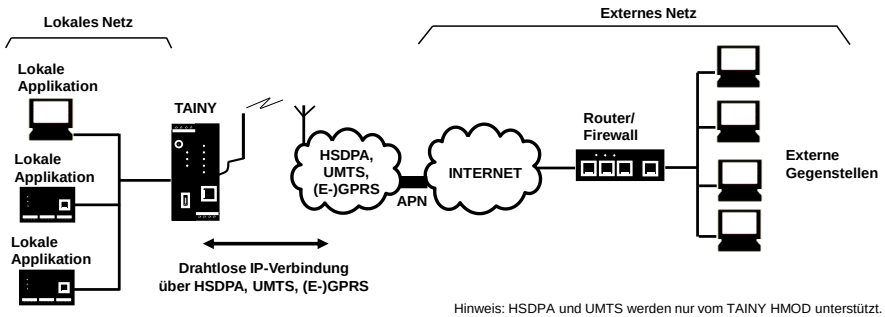
Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Szenarium 2: Verbindung über HSDPA, UMTS, EGPRS oder GPRS und ein direktes VPN des Mobilfunkbetreibers zum externen Netz:



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Szenarium 3: Verbindung über HSDPA, UMTS, EGPRS oder GPRS und das Internet zum externen Netz:



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Lokale Applikationen könnten zum Beispiel eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, oder ein Notebook bzw. PC sein. Diese Applikationen benutzen das TAINY xMOD, um Zugriff auf ein externes Netz zu erhalten, so als wenn sie direkt vor Ort an diesem externen Netz angeschlossen wären.

Funktionen

Um die Aufgaben in den beschriebenen Szenarien zu erfüllen, vereinigen die Geräte je nach Ausführung folgende Funktionen:

	TAINY HMOD		TAINY EMOD	
	V2-IO	L1-IO	V2-IO	L1-IO
HSDPA / UMTS	X	X	-	-
EGPRS / GPRS / CSD	X*)	X*)	X	X
VPN-Funktionen	X	-	X	-
Firewall	X	X	X	X
Konfiguration	X	X	X	X
Weitere Funktionen	X	X	X	X

*) CSD nur, wenn nicht in einem HSDPA / UMTS Netz eingebucht

Kommunikation

Funkmodem für die flexible Datenkommunikation in UMTS-Netzen

- per HSDPA, UMTS

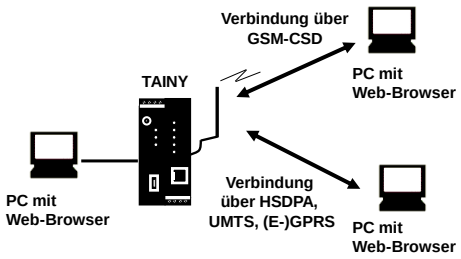
Funkmodem für die flexible Datenkommunikation in GSM-Netzen

- EGPRS, GPRS (und CSD)

Konfiguration

Die Konfiguration des Gerätes erfolgt über eine Web-Oberfläche die sich einfach mit einem Web-Browser anzeigen lässt. Der Zugriff kann über folgende Wege stattfinden:

- die lokale Schnittstelle,
- HSDPA, UMTS, EGPRS, GPRS oder
- CSD (Circuit Switched Data = Datenwählverbindungen) des GSM



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

VPN-Funktionen

Das TAINY HMOD-V2-IO sowie das TAINY EMOD-V2-IO bieten folgende VPN-Features

- VPN-Router für sichere Datenübertragung über öffentliche Netze
- Protokoll: IPsec (Tunnelmode)
- IPsec-3DES-Verschlüsselung mit 192 Bit
- IPsec-AES-Verschlüsselung mit 128, 192 und 256 Bit
- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Agressive Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate, CA
- NAT-T
- 1-zu-1-NAT
- Dead Peer Detection (DPD)
- Schaltausgang zur Anzeige eines aufgebauten VPN-Tunnels

Firewall

Die TAINY xMOD bieten folgende Firewall-Funktionen um das lokale Netz und sich selbst gegen Angriffe von außen zu schützen:

- Stateful Inspection Firewall
- Anti-Spoofing
- Port Forwarding

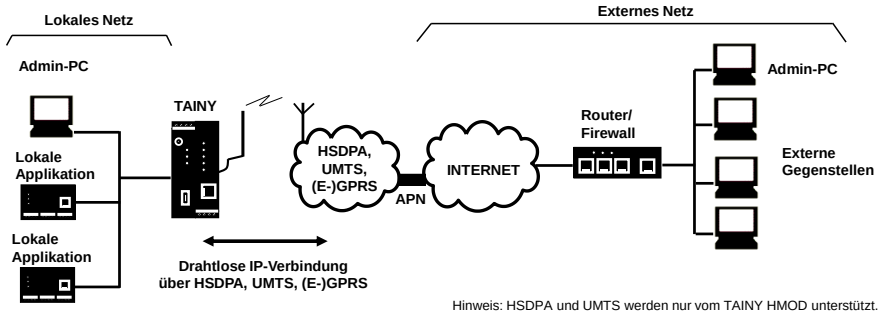
Weitere Funktionen

Die TAINY xMOD bietet folgende weitere Funktionen:

- DNS Cache
- DHCP-Server
- NTP
- Remote Logging
- Schalteingang
- Web-Oberfläche zur Konfiguration
- Versand von Alarm-SMS
- Versand von SNMP-Traps
- SMS-Versand aus dem lokalen Netz
- SSH-Konsole zur Konfiguration
- SNMP zur Kontrolle und Konfiguration
- DynDNS-Client
- Datenwählverbindung zur Wartung und Fernkonfiguration
- Volumenüberwachung
- Installationsmodus zur Antennenausrichtung

Begriffe

Häufig verwendete Begriffe in diesem Handbuch werden an dieser Stelle festgelegt:



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Lokales Netz

Netzwerk, angeschlossen an der lokalen Schnittstelle der TAINY xMOD. Das lokale Netz enthält mindestens eine lokale Applikation.

Lokale Schnittstelle

Schnittstelle der TAINY xMOD zum Anschluss des lokalen Netzes. Die Schnittstelle ist am Gerät mit 10/100-Base-T gekennzeichnet. Es handelt sich um eine Ethernet-Schnittstelle mit 10Mbit/s oder 100Mbit/s Datenrate (Autosensing MDI/MDIX).

Lokale Applikation

Lokale Applikationen sind Netzwerkkomponenten im lokalen Netz, zum Beispiel eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC oder der Admin-PC.

Admin-PC

Rechner mit Web-Browser (z.B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version 2) angeschlossen an das lokale Netz oder das externe Netz, mit dem die Konfiguration der TAINY xMOD durchgeführt wird. Der Web-Browser muss HTTPS unterstützen. Für die Gerätekonfiguration über SSH wird auf dem Admin-PC ein SSH-Client, wie z.B. putty benötigt.

Externes Netz

Externes Netzwerk, mit dem das TAINY HMOD über HSDPA, UMTS, EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet.

Externes Netzwerk, mit dem das TAINY EMOD über EGPRS oder GPRS verbunden ist. Externe Netze sind das Internet oder ein privates Intranet

Externe Gegenstellen

Externe Gegenstellen sind Netzwerkkomponenten im externen Netz, z.B. Web-Server im Internet, Router im Intranet, ein zentraler Firmenserver, ein Admin-PC und vieles mehr.

(E-)GPRS

EGPRS oder GPRS, je nach Verfügbarkeit der Dienste.

VPN-Gateway

Komponente des externen gegenüberliegenden Netzes, die IPsec unterstützt und kompatibel ist zum TAINY xMOD-V2-IO.

Gegenüberliegendes Netz

Externes Netz, mit dem das TAINY xMOD eine VPN-Verbindung aufbaut.

Mobilfunknetz

Infrastruktur und Technologie zur drahtlosen mobilen Sprach- und Datenkommunikation.

Das TAINY HMOD ist für den Einsatz in UMTS-Mobilfunknetzen und GSM-Mobilfunknetzen gebaut,

Das TAINY EMOD ist für den Einsatz in EDGE-/GSM-Mobilfunknetzen gebaut.

Datenfunkdienst

Vom verwendeten Mobilfunknetz bereitgestellte Dienste zur Datenübertragung, die vom TAINY xMOD genutzt werden können:

	TAINY HMOD		TAINY EMOD	
	V2-IO	L1-IO	V2-IO	L1-IO
UMTS-Mobilfunknetz	X	X	-	-
HSDPA	X	X	-	-
UMTS data	X	X	-	-
GSM-Mobilfunknetz (mit EDGE)	X	X	X	X
E-GPRS	X	X	X	X
GPRS	X	X	X	X
CSD	X*)	X*)	X	X

*) CSD nur, wenn nicht in einem HSDPA / UMTS Netz eingebucht

2 Inbetriebnahme

2.1 Schritt für Schritt

Gehen Sie bei der Inbetriebnahme des TAINY xMOD bitte in folgenden Schritten vor:

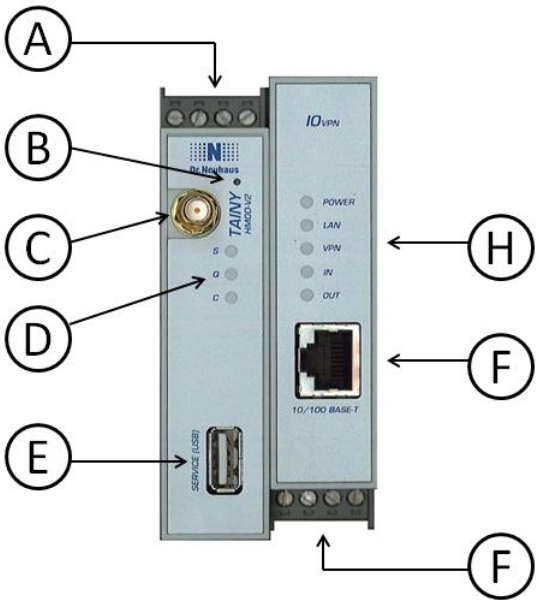
Schritt		Kapitel
1.	Machen Sie sich bitte zunächst mit den Voraussetzungen für den Betrieb des TAINY xMOD vertraut.	2.2
2.	Lesen Sie bitte sehr sorgfältig die Sicherheitshinweise und weitere Hinweise am Beginn dieses Anwenderhandbuches und befolgen Sie diese bitte unbedingt.	
3.	Machen Sie sich bitte vertraut mit den Bedienelementen, Anschlüssen und Betriebsanzeigen des TAINY xMOD.	2.3 bis 2.6
4.	Schließen Sie einen PC mit Web-Browser (Admin-PC) an die lokale Schnittstelle (10/100 BASE-T) des TAINY xMOD an.	3.3, 3.4
5.	Tragen Sie über die Web-Oberfläche des TAINY xMOD die PIN (Persönliche Identifikations-Nummer der SIM-Karte ein).	5.1
6.	Trennen Sie das TAINY xMOD wieder von der Versorgungsspannung.	2.6
7.	Legen Sie die SIM-Karte in das Gerät ein.	2.7
8.	Schließen Sie die Antenne an.	2.6
9.	Verbinden Sie das TAINY xMOD mit der Versorgungsspannung.	2.6
10.	Richten Sie das TAINY xMOD nach Ihren Anforderungen ein.	3 bis 11
11.	Schließen Sie Ihre lokale Applikation an.	2.6

2.2 Voraussetzungen für den Betrieb

Um das TAINY xMOD betreiben zu können, müssen die folgenden Informationen vorliegen und die folgenden Voraussetzungen erfüllt sein:

Antenne	Eine Antenne, angepasst auf die Frequenzbänder des von Ihnen gewählten UMTS/GSM-Mobilfunknetzes: 850 MHz, 900 MHz, 1800 MHz, 1900 MHz oder 2100 MHz. Verwenden Sie bitte Antennen aus dem Zubehör zum TAINY xMOD, da diese für den Betrieb mit den Geräten geprüft sind. Siehe Kapitel 2.6.
Spannungsversorgung	Eine Spannungsversorgung mit einer Spannung zwischen 12 V_{DC} und 60 V_{DC}, die einen ausreichenden Strom liefern kann (I_{Burst} > 1,26 A). Siehe Kapitel 2.6 und Kapitel 13.
SIM-Karte	Eine SIM-Karte des ausgewählten Mobilfunkbetreibers.
PIN	Die PIN der SIM-Karte
HSDPA / UMTS/ EGPRS / GPRS Freischaltung	Die SIM-Karte muss von Ihrem Mobilfunk-Netzbetreiber für die Dienste HSDPA, UMTS data (nur TAINY HMOD) und / oder EGPRS oder GPRS freigeschaltet sein. Die Zugangsdaten müssen bekannt sein: - Access Point Name (APN) - Benutzername - Passwort
CSD 9600 bit/s Freischaltung	Die SIM-Karte muss von Ihrem Mobilfunk-Netzbetreiber für den CSD-Dienst freigeschaltet sein, wenn Sie die Fernkonfiguration über Datenwählverbindungen, siehe Kapitel 8.3, nutzen möchten.

2.3 Überblick



A – Anschlussklemmen der Stromversorgung

B – Service-Taster

C – Antennenbuchse Typ SMA

D – Betriebsanzeigen S, Q, C

E – Service (USB) – Reserviert für spätere Anwendungen

F – Anschlussklemmen des Schalteingang und Schaltausgangs

G – 10/100-Base-T - RJ45-Buchse zum Anschluss des lokalen Netzes

H – Betriebsanzeigen
POWER, LAN, IN, OUT
VPN (nur TAINY xMOD-V2-IO)

2.4 Service-Taster

Auf der Frontseite des TAINY xMOD befindet sich ein kleines Loch (siehe B), hinter dem sich ein Taster befindet. Benutzen Sie einen dünnen Gegenstand, z.B. eine aufgebogene Büroklammer, um den Taster zu drücken

- Wenn Sie den Taster länger als 5 sec drücken, führt das TAINY xMOD einen Neustart durch und lädt dabei die Werkseinstellungen.

2.5 Betriebsanzeigen

Das TAINY xMOD-V2-IO hat jeweils 8 Signalleuchten (LEDs), das TAINY xMOD-L1-IO hat 7 Signalleuchten (LEDs) zur Anzeige des Betriebszustands.

Die 3 Signalleuchten auf der linken Gerätehälfte zeigen den Zustand des Funkmodems an:

TAINY HMOD

Leuchte	Zustand	Bedeutung
***S** (Status)*	Langsam blinkend	PIN-Übergabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	EIN	PIN-Übergabe erfolgreich
***Q** (Quality)*	AUS	Nicht im GSM-Netz eingebucht
	Kurz aufblinkend	Signalstärke schlecht (CSQ < 6)
	Langsam blinkend	Signalstärke mittel (CSQ= 6..10)
	EIN mit kurzen Unterbrechungen	Signalstärke gut (CSQ=11-18)
	EIN	Signalstärke sehr gut (CSQ > 18)
***C** (Connect)*	AUS	Keine Verbindung
	Schnell blinkend	Service-Ruf über CSD aktiv
	Langsam blinkend	EGPRS/GPRS-Verbindung aktiv
	EIN	HSDPA/UMTS-Verbindung aktiv
S, Q, C gemeinsam	schnelles Lauflicht	Booten
	langsames Lauflicht	Update
	synchrones schnelles Blinken	Fehler

TAINY EMOD

Leuchte	Zustand	Bedeutung
S *(Status)*	Langsam blinkend	PIN-Übergabe
	Schnell blinkend	PIN-Fehler / SIM-Fehler
	EIN	PIN-Übergabe erfolgreich
Q *(Quality)*	AUS	Nicht im GSM-Netz eingebucht
	Kurz aufblinkend	Signalstärke schlecht (CSQ < 6)
	Langsam blinkend	Signalstärke mittel (CSQ= 6..10)
	EIN mit kurzen Unterbrechungen	Signalstärke gut (CSQ=11-18)
	EIN	Signalstärke sehr gut (CSQ > 18)
C *(Connect)*	AUS	Keine Verbindung
	Schnell blinkend	Service-Ruf über CSD aktiv
	EIN mit kurzen Unterbrechungen	GPRS-Verbindung aktiv
	EIN	EGPRS-Verbindung aktiv
S, Q, C gemeinsam	schnelles Lauflicht	Booten
	langsames Lauflicht	Update
	synchrones schnelles Blinken	Fehler

TAINY xMOD-V2-IO

Die 5 Signalleuchten auf der rechten Gerätehälfte zeigen den Zustand weiterer Gerätefunktionen an:

Leuchte	Zustand	Bedeutung
POWER	EIN	Gerät eingeschaltet, Betriebsspannung liegt an
	AUS	Gerät ausgeschaltet, Betriebsspannung fehlt
LAN	EIN	Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz hergestellt
	AUS	Keine Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz
	EIN mit kurzen Unterbrechungen	Datentransfer über die Ethernet-Verbindung
VPN	EIN	Mindestens eine VPN-Verbindung aufgebaut
	AUS	Keine VPN-Verbindung aufgebaut
IN	EIN	Schalteingang aktiv
	AUS	Schalteingang nicht aktiv
OUT	EIN	Schaltausgang aktiv
	AUS	Schaltausgang nicht aktiv

TAINY xMOD-L1-IO

Die 4 Signalleuchten auf der rechten Gerätehälfte zeigen den Zustand weiterer Gerätefunktionen an:

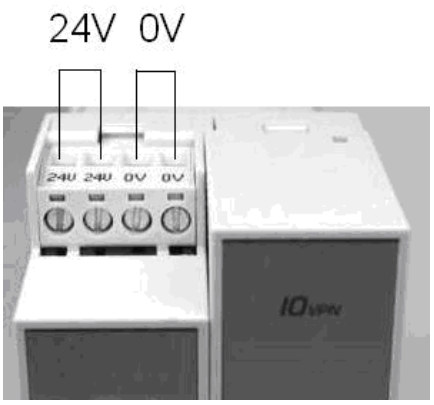
Leuchte	Zustand	Bedeutung
POWER	EIN	Gerät eingeschaltet, Betriebsspannung liegt an
	AUS	Gerät ausgeschaltet, Betriebsspannung fehlt
LAN	EIN	Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz hergestellt
	AUS	Keine Ethernet-Verbindung zur lokalen Applikation bzw. zum lokalen Netz
	EIN mit kurzen Unterbrechungen	Datentransfer über die Ethernet-Verbindung
IN	EIN	Schalteingang aktiv
	AUS	Schalteingang nicht aktiv
OUT	EIN	Reserviert für zukünftige Anwendungen
	AUS	Reserviert für zukünftige Anwendungen

2.6 Anschlüsse

10/100-Base-T	Am Anschluss 10/100-Base-T wird das lokale Netz mit den lokalen Applikationen angeschlossen, z.B. eine programmierbare Steuerung, eine Maschine mit Ethernet-Schnittstelle zur Fernüberwachung, ein Notebook bzw. PC. Zum Einrichten des TAINY xMOD schließen Sie hier den Admin-PC mit Web-Browser an. Die Schnittstelle unterstützt Autonegotiation. Somit wird automatisch erkannt, ob 10 Mbit/s oder 100 Mbit/s Übertragungsgeschwindigkeit auf dem Ethernet genutzt wird. Das verwendete Anschlusskabel muss einen RJ45-Stecker haben. Es kann Cross-over oder Eins-zu-Eins verdrahtet sein (MDI/MDIX).
Service (USB)	Diese Schnittstelle ist beim TAINY xMOD ohne Funktion und reserviert für spätere Anwendungen. Bitte schließen Sie hier keine Geräte an. Der Betrieb des TAINY xMOD könnte gestört werden.
SMA Antennen-Buchse	Das TAINY xMOD hat eine Antennenbuchse vom Typ SMA zum Anschluss der Antenne. Achten Sie darauf, dass im Betrieb immer eine Antenne angeschlossen ist. Die verwendete Antenne soll eine Impedanz von ca. 50 Ohm haben. Sie muss abgestimmt sein für GSM 900MHz und DCS 1800MHz oder GSM 850 MHz und PCS 1900 MHz, oder für UMTS 2100 MHz je nachdem, welche Frequenzbänder ihr UMTS/GSM-Mobilfunkbetreiber verwendet. In Europa und China werden GSM 900MHz, DCS 1800MHz und UMTS 2100MHz verwendet, in den USA verwendet man GSM 850 MHz und PCS 1900 MHz (auch für UMTS). Bitte erkundigen Sie sich bei Ihrem Netzbetreiber. Die Anpassung (VSWR) der Antenne muss 1:2,5 oder besser sein. **Achtung:** Verwenden Sie bitte nur Antennen aus dem Zubehörprogramm für das TAINY xMOD. Diese Antennen sind von uns geprüft und gewährleisten die beschriebenen Produkteigenschaften. Bei der Installation der Antenne ist auf eine ausreichend gute Signalqualität zu achten (CSQ > 11). Nutzen Sie die Signalleuchten des TAINY xMOD, die Ihnen die Signalqualität anzeigen oder den Installationsmodus, siehe Kapitel 5.6. Achten Sie bitte darauf, dass sich keine großen metallischen Gegenstände (z.B. Stahlbeton) in der Nähe der Antenne befinden. Bitte beachten Sie die Montage- und Gebrauchsanleitung der verwendeten Antenne **Warnung:** Bei Außenmontage der Antenne muss die Antenne zwecks Blitzschutzes geerdet werden. Diese Arbeiten müssen von qualifiziertem Personal durchgeführt werden.

Schraubklemmen

Versorgung



Schalteingang/Schaltausgang

24V / 0V Versorgungs-Spannung

Das TAINY xMOD arbeitet mit einer Gleichspannung von 12-60 V DC, nominell 24 V DC. Diese Versorgungsspannung wird an die Schraubklemmen der linken Gerätehälfte angeschlossen.

Die Stromaufnahme beträgt etwa 450mA bei 12V und 100mA bei 60V (I_{Burst} > 1,26 A).

Warnung:

Das Netzteil des TAINY xMOD ist nicht potentialgetrennt.

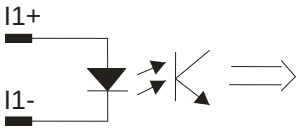
Beachten Sie bitte die Sicherheitshinweise am Anfang dieses Handbuchs.

Hinweis:

Achten Sie bitte auf eine ausreichende Dimensionierung der Versorgungsquelle. Eine zu schwache Versorgung kann zu einem instabilen Betrieb führen.

Schalteingang I1+/ I1-

Das TAINY xMOD hat einen Schalteingang. Der Schalteingang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte. Die Klemmen sind mit I1+/I1- bezeichnet.



U_{In} = 5 …30V; An: $U_{In} \geq$ 5 V; Aus: $U_{In} \leq$ 1,2 V

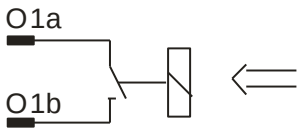
Zur Funktion des Schalteingangs siehe auch Kapitel 9.6.

Warnung:

Der Schalteingang ist gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schalteingangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schalteingangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

Schaltausgang O1a/ O1b

Das TAINY xMOD-V2-IO hat einen Schaltausgang. Der Schaltausgang hat seine Anschlüsse an den Schraubklemmen der rechten Gerätehälfte. Die Klemmen sind mit O1a/O1b bezeichnet.



U_{Max} = 30V; I_{Max} = 20mA

Der Schaltausgang ist aktiv (Schalter geschlossen), wenn mindestens eine VPN-Verbindung aufgebaut ist.

Der Schaltausgang ist nicht aktiv (Schalter offen), wenn keine VPN-Verbindung aufgebaut ist.

Warnung:

Der Schaltausgang ist gegenüber den anderen Anschlüssen des TAINY xMOD galvanisch getrennt. Verbindet die am TAINY xMOD angeschlossene Installation ein Signal des Schaltausgangs galvanisch mit der Versorgungsspannung, darf zwischen jedem Signal des Schaltausgangs und jedem Anschluss der Versorgungsspannung des TAINY xMOD die Spannung jeweils 60V nicht überschreiten.

2.7 Die SIM-Karte einlegen

Achtung:

Bevor Sie die SIM-Karte einlegen, tragen Sie bitte im TAINY xMOD über die Web-Oberfläche die PIN der SIM-Karte ein. Siehe Kapitel 5.1.

1. Nachdem Sie die PIN der SIM-Karte eingetragen haben, trennen Sie bitte das TAINY xMOD vollständig von der Versorgungsspannung.
2. Die Schublade für die SIM-Karte befindet sich auf der Geräterückseite. In der Gehäuseöffnung befindet sich direkt neben der Schublade für die SIM-Karte ein kleiner gelber Taster. Drücken Sie auf diesen Taster mit einem spitzen Gegenstand, z.B. einem Bleistift.

   Bei Druck auf den Taster, kommt die SIM-Karten-Schublade aus dem Gehäuse.
3. Legen Sie die SIM-Karte so in die Schublade, dass ihre vergoldeten Kontakte sichtbar bleiben.
4. Schieben Sie dann bitte die Schublade mit der SIM-Karte vollständig in das Gehäuse.

Achtung!

Legen Sie die SIM-Karte auf keinen Fall im Betrieb ein oder entfernen Sie sie. Die SIM-Karte und das TAINY xMOD könnten beschädigt werden.

3 Konfiguration

3.1 Übersicht

Die Konfiguration der Router- und Firewall-Funktionen erfolgt lokal oder aus der Ferne über die web-basierte Administrations-Oberfläche des TAINY xMOD. Für das TAINY xMOD-V2-IO kann zusätzlich eine Konfiguration der VPN-Funktion erfolgen.

Fernkonfiguration

Eine Fernkonfiguration über HTTPS- oder CSD-Zugang ist nur möglich, sofern das TAINY xMOD für Fernzugriffe konfiguriert ist. Sie gehen in diesem Fall genauso vor, wie in Kapitel 8 beschrieben.

Konfiguration über die lokale Schnittstelle

Die Voraussetzungen für die Konfiguration über die lokale Schnittstelle sind:

- Der Rechner (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss entweder
  - direkt an der Ethernet-Buchse des TAINY xMOD per Netzwerkkabel angeschlossen sein

  oder
  - über das lokale Netz direkten Zugriff auf das TAINY xMOD haben.
- Der Netzwerkadapter des Rechners (Admin-PC), mit dem Sie die Konfiguration vornehmen, muss folgende TCP/IP Konfiguration haben:

  IP-Adresse: **192.168.1.2**

  Subnetzmaske: **255.255.255.0**

  Statt der IP-Adresse **192.168.1.2** können Sie auch andere IP-Adressen aus dem **Bereich 192.168.1.x** verwenden, aber nicht 192.168.1.1, 192.168.1.0 und 192.168.1.255.
- Wenn Sie mit dem Admin-PC über das TAINY xMOD auch auf das externe Netz zugreifen möchten, sind zusätzlich folgende Einstellungen erforderlich:

  Standardgateway: **192.168.1.1**

  Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

3.2 Erlaubte Zeichen bei Benutzernamen, Passwörtern und weiteren Eingaben

Bei Eingaben von Benutzernamen, Passwörtern, Hostnamen, APN und PIN sind folgende darstellbare ASCII-Zeichen erlaubt:

Benutzernamen, Passwörter und PIN

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | }

Hostnamen und APN

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h I j k l m n o p q r s t u v w x y z . -

3.3 TCP/IP Konfiguration des Netzwerkadapters unter Windows XP

Windows Verbinden mit…

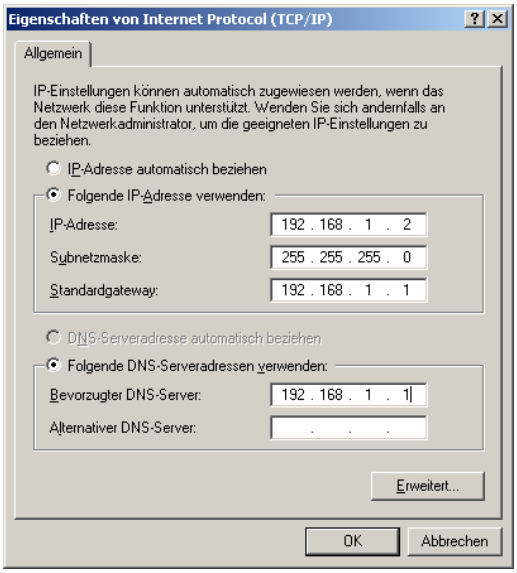
Klicken Sie *Start, Verbinden mit ..., Alle Verbindungen anzeigen…*

Klicken Sie dann auf *LAN-Verbindung.* Wählen sie im Dialogfeld *Eigenschaften von LAN-Verbindung* die Registerkarte *Allgemein* und markieren Sie dort den Eintrag *Internetprotokoll (TCP/IP).* Öffnen Sie *Eigenschaften* durch klicken auf diese Schaltfläche.

Es erscheint das Fenster *Eigenschaften von Internetprotokoll TCP/IP* (siehe Abbildung unten).

Hinweis:

Der Weg der zum Dialogfeld *Eigenschaften von LAN-Verbindung* führt hängt von Ihren Windows Einstellungen ab. Können Sie das Dialogfeld nicht finden, suchen Sie bitte in der Windows-Hilfe nach *LAN-Verbindung* oder *Eigenschaften von Internetprotokoll TCP/IP*.


Eigenschaften von Internet Protocol (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server: 192 . 168 . 1 . 1
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Geben Sie folgende Werte ein, um die Web-Oberfläche des TAINY xMOD zu erreichen:

IP-Adresse: **192.168.1.2**

Subnetzmaske: **255.255.255.0**

Geben Sie zusätzlich folgende Werte ein, wenn Sie mit dem Admin-PC über das TAINY xMOD auf das externe Netz zugreifen wollen:

Standardgateway: **192.168.1.1**

Bevorzugter DNS-Server: **Adresse des Domain Name Servers**

Bevorzugter DNS-Server

Wenn Sie Adressen über einen Domain-Namen aufrufen (z. B. www.neuhaus.de), dann muss auf einem Domain Name Server (DNS) nachgeschlagen werden, welche IP-Adresse sich hinter dem Namen verbirgt. Als Domain Name Server können Sie festlegen:

- DNS-Adresse des Netzbetreibers

  oder

- Lokale IP-Adresse des TAINY xMOD, sofern dieses zum Auflösen von Hostnamen in IP-Adressen konfiguriert ist (siehe Kapitel 4.3). Dies ist die **Werkseinstellung**.

Um den Domain Name Server in der TCP/IP-Konfiguration Ihres Netzwerkadapters festzulegen, gehen Sie wie oben beschrieben vor.

3.4 Konfigurations-Verbindung herstellen

Web-Browser einrichten

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.

   (z.B. MS Internet Explorer ab Version 7 oder Mozilla Firefox ab Version 2; der Web-Browser muss SSL (d. h. HTTPS) unterstützen.)

2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt.

   Im MS Internet Explorer 7 nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Die Option *Keine Verbindung wählen* muss aktiviert sein.

Startseite des TAINY xMOD aufrufen

3. In der Adresszeile des Browsers geben Sie die Adresse TAINY xMOD vollständig ein. Gemäß Werkseinstellung lautet diese:

   https://192.168.1.1

   Folge: Es erscheint ein Sicherheitshinweis. Beim Internet Explorer 7 zum Beispiel dieser:

Sicherheitshinweis bestätigen

Es besteht ein Problem mit dem Sicherheitszertifikat der Website.
Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.
Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.
Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.
Klicken Sie hier, um diese Webseite zu schließen.
Laden dieser Website fortsetzen (nicht empfohlen).
Weitere Informationen

4. Quittieren Sie den entsprechenden Sicherheitshinweis mit „Laden dieser Webseite fortsetzen …“

Hinweis

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst unterzeichneten Zertifikat ausgeliefert. Bei Zertifikaten mit Unterschriften, die dem Betriebssystem nicht bekannt sind, erfolgt ein Sicherheitshinweis. Sie können sich das Zertifikat anzeigen lassen.
Aus dem Zertifikat muss erkenntlich sein, dass es für Dr. Neuhaus Telekommunikation GmbH ausgestellt wurde. Die Web-Oberfläche wird über eine IP-Adresse adressiert und nicht über einen Namen, daher stimmt der im Sicherheitszertifikat angegebene Name nicht mit dem im Zertifikat überein.

5. Sie werden aufgefordert, den Benutzernamen und das Passwort (Kennwort) anzugeben:

Benutzername und Passwort eingeben

Die werkseitige Voreinstellung lautet:

Benutzername: **root**

Kennwort: **root**

Hinweis

Sie sollten auf jeden Fall das Passwort (Kennwort) ändern. Die werkseitige Voreinstellung ist allgemein bekannt und ist kein ausreichender Schutz. Im Kapitel 3.8 ist beschrieben, wie das Passwort geändert werden kann.

Die Startseite wird angezeigt

Nach Eingabe von Benutzernamen und Passwort erscheint im Web-Browser die Startseite des TAINY xMOD mit einem Überblick über den Betriebszustand, siehe Kapitel 3.5.

Die Startseite wird nicht angezeigt

Sollte auch nach wiederholtem Versuch der Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Überprüfen Sie die Hardware-Verbindung. Dazu bei einem Windows-Rechner über die DOS-Eingabeaufforderung (Menü *Start, Programme, Zubehör, Eingabeaufforderung*) folgenden Befehl eingeben:

  ping 192.168.1.1

  Wenn innerhalb der vorgegebenen Zeitspanne die Meldung über den Rück-Empfang der 4 ausgesendeten Pakete nicht erscheint, überprüfen Sie bitte das Kabel, die Anschlüsse und die Netzwerkkarte.

- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet. Im MS Internet Explorer (Version 7.0) nehmen Sie diese Einstellung wie folgt vor: Menü *Extras, Internetoptionen...*, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche *Einstellungen...* klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter *Proxyserver* der Eintrag *Proxyserver für LAN verwenden* nicht aktiviert ist.

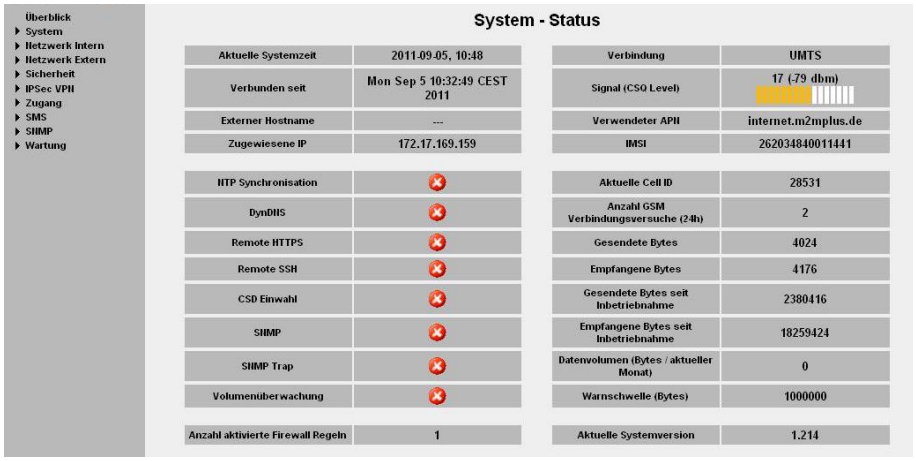
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü *Start, Verbinden mit ..., Systemsteuerung, Alle Verbindungen anzeigen* unter LAN oder Höchstgeschwindigkeits-Internet die betreffende Verbindung mit der rechten Maustaste klicken und im Kontextmenü *Deaktivieren* wählen.

- Geben Sie die Adresse des TAINY xMOD mit Slash ein:

  https://192.168.1.1/

3.5 System Status (Startseite)

System Status



Nach Aufrufen der Web-Oberfläche des TAINY xMOD und der Eingabe von Benutzernamen und Passwort erscheint ein Überblick über den aktuellen Betriebszustand des Gerätes.

Hinweis

Benutzen Sie die Funktion *Aktualisieren* des Web-Browsers um die angezeigten Werte auf den aktuellen Stand zu bringen.

Aktuelle Systemzeit	Zeigt die aktuelle Systemzeit des TAINY xMOD an, im Format: Jahr – Monat – Tag, Stunden – Minuten
Verbunden seit	Zeigt an, wie lange die aktuelle Verbindung zum Datenfunkdienst besteht.
Externer Hostname	Zeigt den Hostnamen (z.B. tainy.mydns.org) des TAINY xMOD an, wenn ein DynDNS-Dienst verwendet wird.
Zugewiesene IP-Adresse	Zeigt die IP-Adresse an, unter der das TAINY xMOD über den Datenfunkdienst zu erreichen ist. Diese IP-Adresse wird dem TAINY xMOD vom Datenfunkdienst zugewiesen.
Verbindung	Zeigt an ob, und welche Funkverbindung besteht. Bei TAINY HMOD: - UMTS-Verbindung (IP-Verbindung über HSDPA, UMTS data) - GPRS/EDGE-Verbindung (IP-Verbindung über EGPRS oder GPRS) - CSD-Verbindung (Service-Verbindung über CSD) Bei TAINY EMOD: - EDGE-Verbindung (IP-Verbindung über EGPRS) - GPRS-Vebindung (IP-Verbindung über GPRS) - CSD-Verbindung (Service-Verbindung über CSD)

Hinweis

Es kann vorkommen, dass eine Funkverbindung und auch eine zugewiesene IP-Adresse angezeigt werden, die Verbindungsqualität aber dennoch nicht ausreicht um Daten zu übertragen. Aus diesem Grunde empfehlen wir, die aktive Verbindungsüberwachung (siehe Kapitel 5.2) zu nutzen.

Signal (CSQ Level)	Gibt die Stärke des GSM-Signals als CSQ-Wert und (in Klammern) als RSSI-Wert in dBm an. □ CSQ < 6: Signalstärke schlecht □ CSQ= 6..10: Signalstärke mittel □ CSQ=11-18: Signalstärke gut □ CSQ > 18: Signalstärke sehr gut □ CSQ = 99: Keine Verbindung zum Funknetz
Verwendeter APN	Zeigt den verwendeten APN (= Access Point Name) des Datenfunkdienstes an.
IMSI	Zeigt die Teilnehmerkennung an, die auf der verwendeten SIM-Karte gespeichert ist. Anhand der IMSI (= International Mobile Subscriber Identity) erkennt der GSM-Netzbetreiber die Berechtigungen und vereinbarten Dienste der SIM-Karte.
NTP-Synchronisation	Zeigt an, ob die NTP-Synchronisation aktiviert ist. NTP-Synchronisation aktiviert. NTP-Synchronisation nicht aktiviert
DynDNS	Zeigt an, ob ein DynDNS-Dienst aktiviert ist. DynDNS-Dienst aktiviert. DynDNS-Dienst nicht aktiviert
Remote HTTPS	Zeigt an, ob Zugriffe auf die Web-Oberfläche des TAINY xMOD aus der Ferne über den Datenfunkdienst erlaubt sind (siehe Kapitel 8.1). Der Zugriff per HTTPS ist erlaubt. Der Zugriff per HTTPS ist nicht erlaubt.
Remote SSH	Zeigt an, ob Zugriffe auf die SSH-Konsole des TAINY xMOD aus der Ferne über den Datenfunkdienst erlaubt sind (siehe Kapitel 8.2). Der Zugriff per SSH ist erlaubt. Der Zugriff per SSH ist nicht erlaubt.
CSD-Einwahl	Zeigt an, ob CSD-Serviceanrufe aus der Ferne erlaubt sind. CSD-Serviceanrufe sind möglich. CSD-Serviceanrufe sind nicht möglich.
SNMP	Zeigt an, ob das Setzen und Lesen von Parametern per SNMP freigegeben ist (siehe Kapitel 11.1): Setzen/Lesen von Parametern per SNMP ist erlaubt. Setzen/Lesen von Parametern per SNMP ist nicht erlaubt.
SNMP-Trap	Zeigt an, ob das Versenden von SNMP-Benachrichtigungen (SNMP-Traps) freigegeben ist (siehe Kapitel 11.2): Versand von SNMP-Benachrichtungen aktiviert. SNMP-Benachrichtungen nicht aktiviert.
Volumenüberwachung	Zeigt an, ob die Volumenüberwachung eingeschaltet ist (siehe Kapitel 5.7): Volumenüberwachung ist aktiviert. Volumenüberwachung ist nicht aktiviert.

Aktuelle Cell ID	Zeigt die Kennung der Mobilfunk-Basisstation an, mit der das TAINY xMOD derzeit verbunden ist.
Anzahl GSM-Verbindungsversuche (24h)	Zeigt die Anzahl der Anmeldeversuche des TAINY xMOD am APN seit 0:00 Uhr (Systemzeit) an. Der Wert 0 zeigt an, dass kein erneuter Anmeldeversuch stattgefunden hat.
Gesendete Bytes / Empfangene Bytes	Zeigt die Anzahl der Bytes an, die während der bestehenden Verbindung über den Datenfunkdienst gesendet bzw. empfangen worden sind. Die Zähler werden bei Aufbau einer neuen Verbindung zurückgesetzt.
	Hinweis Diese Zahlen dienen nur als Anhaltspunkt für das Datenvolumen und können von der Abrechnung des Netzbetreibers abweichen.
Gesendete Bytes / Empfangene Bytes seit Inbetriebnahme	Zeigt die Anzahl der Bytes an, die seit dem letzten Laden der Werkseinstellung über den Datenfunkdienst gesendet bzw. empfangen worden sind. Die Zähler werden bei Laden der Werkseinstellung zurückgesetzt.
Datenvolumen (Bytes / aktueller Monat)	Zeigt die Anzahl der gesendeten und empfangenen Bytes seit Monatsbeginn (Systemzeit) an.
	Hinweis Diese Zahlen dienen nur als Anhaltspunkt für das Datenvolumen und können von der Abrechnung des GSM-Netzbetreibers deutlich abweichen. Die NTP-Synchronisation muss aktiviert sein.
Warnschwelle (Bytes)	Zeigt die eingestellte Warnschwelle des Datenvolumens an, bei der das TAINY xMOD eine Benachrichtigung versendet.
Anzahl aktivierter Firewall-Regeln	Zeigt an wie viele Firewall-Regeln aktiviert sind.
Aktuelle Systemversion	Zeigt die Versionsnummer der Software des TAINY xMOD an.

3.6 Konfiguration vornehmen

Zur Konfiguration gehen Sie wie folgt vor:

Konfiguration durchführen

1. Per Menü den gewünschten Einstellbereich aufrufen
2. auf der betreffenden Seite die gewünschten Einträge machen oder mit **Zurücksetzen** die aktuelle, nicht gespeicherte Eingabe wieder löschen.
3. mit **Speichern** bestätigen, so dass die Einstellungen vom Gerät übernommen werden.

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO

Hinweis zum Funktionsumfang

Der Menüpunkt IPsec-VPN findet sich nur beim TAINY HMOD-V2-IO und TAINY EMOD-V2-IO.

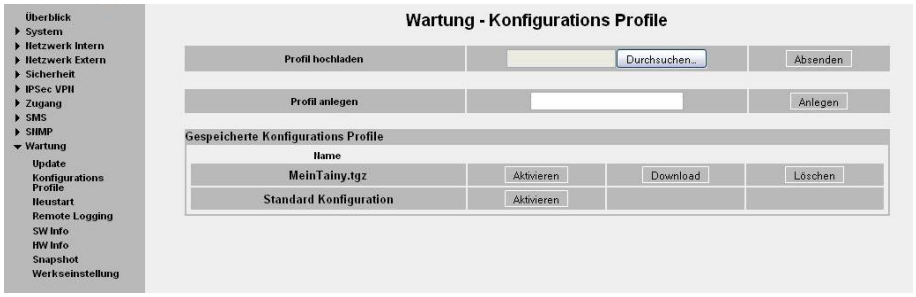
- Je nachdem, wie Sie das TAINY xMOD konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.
- Tragen Sie bei der Eingabe von IP-Adressen, die IP-Adress-Teilnummern immer ohne führende Nullen ein, z.B.: 192.168.0.8.

Fehleingaben

Das TAINY xMOD prüft Ihre Eingaben. Grobe Fehler werden beim Speichern erkannt und das betroffene Eingabefeld wird markiert. Der eingetragene Wert wird auf den Default-Wert zurückgesetzt.

3.7 Konfigurations-Profile

Wartung > Konfigurations-Profile



Funktion

Die Einstellungen des TAINY xMOD können in Konfigurations-Profilen (Dateien) gespeichert und jederzeit neu geladen werden.

Profil hochladen

Lädt ein zuvor erstelltes und auf den Admin-PC gespeichertes Konfigurations-Profil in das TAINY xMOD. Dateien mit Konfigurations-Profilen haben die Dateiendung *.tgz.

Mit *Durchsuchen* können Sie auf dem Admin-PC nach Konfigurations-Profilen suchen,

mit *Absenden* laden Sie das Konfigurations-Profil in das TAINY xMOD.

Es wird dann in der Tabelle der gespeicherten Konfigurations-Profile angezeigt.

Profil anlegen

Speichert die aktuellen Einstellungen des TAINY xMOD in einem Konfigurations-Profil.

Geben Sie zunächst einen Namen für das Profil in dem Eingabefeld ein.

Für den Namen dürfen folgende Zeichen verwendet werden:

( ) . - 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ ] _ a b c d e f g h I j k l m n o p q r s t u v w x y z

Mit *Anlegen* werden die Einstellungen in einem Profil mit diesem Namen gespeichert und dann in der Tabelle der gespeicherten Konfigurations-Profile angezeigt.

Gespeicherte Konfigurations-Profile

Die Tabelle der gespeicherten Konfigurations-Profile zeigt alle Profile an, die in dem TAINY xMOD gespeichert sind.

Download Lädt das Profil auf den Admin-PC.

Aktivieren	Das TAINY xMOD übernimmt die Einstellungen des ausgewählten Konfigurations-Profils und arbeitet mit diesen weiter.
Löschen	Das Konfigurations-Profil wird gelöscht. Das Profil *Standard Konfiguration* enthält die Werkseinstellungen und kann nicht gelöscht werden.

Konfigurations-Profile per SSH laden und aktivieren.

Konfigurations-Profile können auch über den SSH-Zugang (siehe Kapitel 8.2) in das TAINY xMOD geladen und aktiviert werden.

Kopieren Sie dazu das Konfigurations-Profil (z.B. TAINY.tgz) per SSH in das Verzeichnis /webserver/profiles/.

Kopieren Sie danach eine Trigger-Datei mit folgenden Namen in das gleiche Verzeichnis:

<Konfigurations-Profil>@now.trigger

Sobald das TAINY xMOD diese Datei in dem Verzeichnis erkennt, wird das neue Konfigurations-Profil übernommen. Der Inhalt der Trigger-Datei spielt keine Rolle.

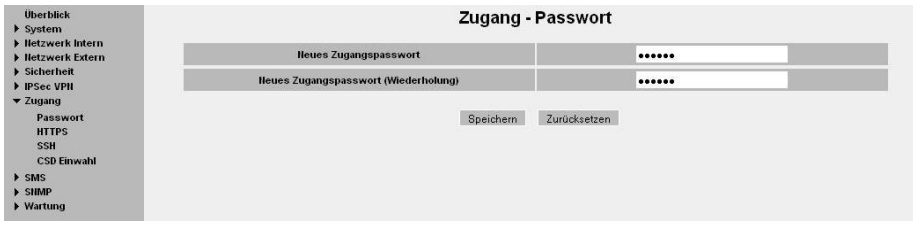
Beispiel:

Konfigurations-Profil: TAINY.tgz

Trigger-Datei: TAINY.tgz@now.trigger

3.8 Passwort ändern

Zugang > Passwort



Funktion

Der Zugang zum TAINY xMOD ist durch ein Zugangspasswort geschützt. Dieses Zugangspasswort schützt sowohl den Zugang über die

- lokale Schnittstelle auf die Web-Oberfläche und
- lokale Schnittstelle auf die SSH-Konsole

wie auch den Zugang über die verfügbare Funkverbindung (HSDPA, UMTS, EGPRS oder GPRS)

- per https auf die Web-Oberfläche und
- per ssh auf die SSH-Konsole

Zugangspasswort (Werkseinstellung)

Die Werkseinstellung für das TAINY xMOD lautet:

- Passwort: *root*
- Benutzername: *root (*kann nicht verändert werden)

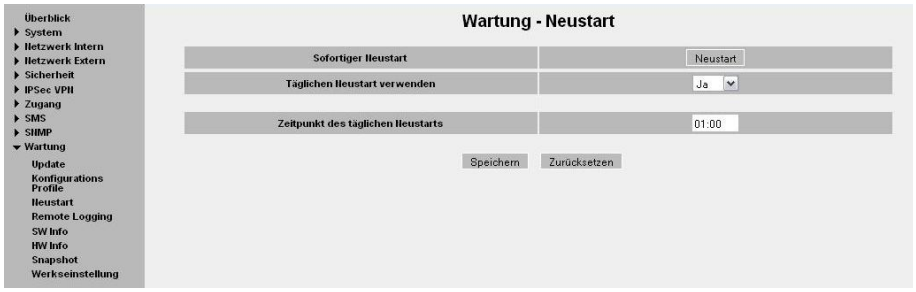
Hinweis

Bitte ändern Sie das Passwort sofort nach Inbetriebnahme. Die werkseitige Voreinstellung ist allgemein bekannt und bietet keinen ausreichenden Schutz.

Neues Zugangspasswort (mit Wiederholung)	Um das Passwort zu ändern, geben Sie bei *Neues Zugangspasswort* das neu ausgewählte Passwort ein und wiederholen Sie die Eingabe im Feld *Neues Zugangspasswort (Wiederholung).* Mit *Zurücksetzen* werden Ihre noch nicht gespeicherten Eingaben verworfen. Mit *Speichern* wird das neue Passwort übernommen.

3.9 Neustart

Wartung > Neustart



Funktion	Obwohl das TAINY xMOD für den Dauerbetrieb ausgelegt ist, kann es bei solch einem komplexen System zu Störungen kommen, oftmals ausgelöst durch äußere Einwirkung. Ein Neustart kann diese Störungen beheben. Der Neustart setzt die Funktionen des TAINY xMOD zurück. Aktuelle Einstellungen entsprechend des Konfigurations-Profils ändern sich nicht. Nach dem Neustart arbeitet TAINY xMOD mit diesen Einstellungen weiter.
Sofortiger Neustart	Der Neustart wird sofort ausgeführt, wenn Sie auf *Neustart* klicken.
Täglichen Neustart verwenden	Der Neustart wird automatisch einmal am Tag ausgeführt, wenn Sie die Funktion mit *Ja* einschalten. Geben Sie den *Zeitpunkt des täglichen Neustarts* an. Der Neustart erfolgt bei der angegebenen Systemzeit. Bestehende Verbindungen werden unterbrochen.
Werkseinstellung	Täglichen Neustart verwenden: **Nein** Zeitpunkt des täglichen Neustarts: **01:00**

3.10 Werkseinstellung laden

Wartung > Werkseinstellung

Zurücksetzen auf Werkskonfiguration	Das Betätigen der Schaltfläche *Zurücksetzen* lädt die werkseitigen Einstellungen, setzt die Passwörter zurück und löscht die gespeicherten Konfigurations-Profile und die archivierten Logbücher. Das TAINY HMOD-V2-IO und das TAINY EMOD-V2-IO löschen zusätzlich die gepeicherten Zertifikate.
Service-Taster	Das Zurücksetzen auf Werkseinstellungen kann auch über den Service-Taster ausgelöst werden (siehe Kapitel 2.4).

Standard Konfiguration	Wenn nur die werkseitigen Einstellungen geladen werden sollen, ohne dass die Konfigurations-Profile und die archivierten Logbücher gelöscht werden, aktivieren Sie nur die Standard-Konfiguration wie in Kapitel 3.7 beschrieben. Für das TAINY HMOD-V2-IO und das TAINY EMOD-V2-IO gilt dieser Vorgang auch für die Zertifikate.

3.11 Geräteidentifikation

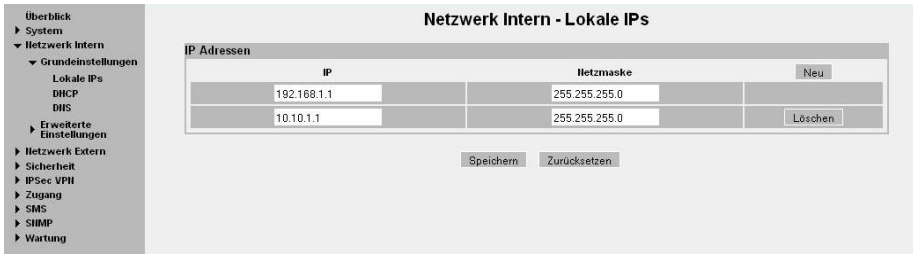
System – Geräteidentifikation

Geräteidentifikation – Zeile 1 - 4	Das TAINY xMOD bietet vier Textfelder, in denen beliebige Zeichenketten zum Beispiel zur Geräteidentifikation gespeichert werden können. Die Textfelder können beschrieben und gelesen werden. Die Textfelder sind jeweils auf 60 Zeichen begrenzt.
Zeichensatz	! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | }
SNMP	Die vier Textfelder können mittels SNMP ausgelesen werden (siehe Kapitel 11.1).

4 Lokale Schnittstelle

4.1 IP-Adressen der lokalen Schnittstelle

Netzwerk Intern > Grundeinstellungen > Lokale IPs

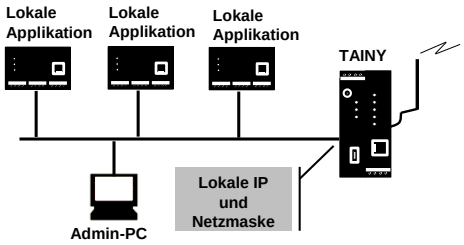


Lokale IP-Adresse laut Werkseinstellung: **192.168.1.1**

An dieser Stelle werden die IP-Adressen und die Netzmasken eingestellt unter denen das TAINY xMOD von lokalen Applikationen erreichbar ist. Werkseitig hat das TAINY xMOD folgende Einstellungen:

IP	192.168.1.1
Netzmaske	255.255.255.0

Diese werkseitig eingestellte IP-Adressen und Netzmaske kann frei verändert werden, sollten jedoch den geltenden Empfehlungen (RFC 1918) folgen.



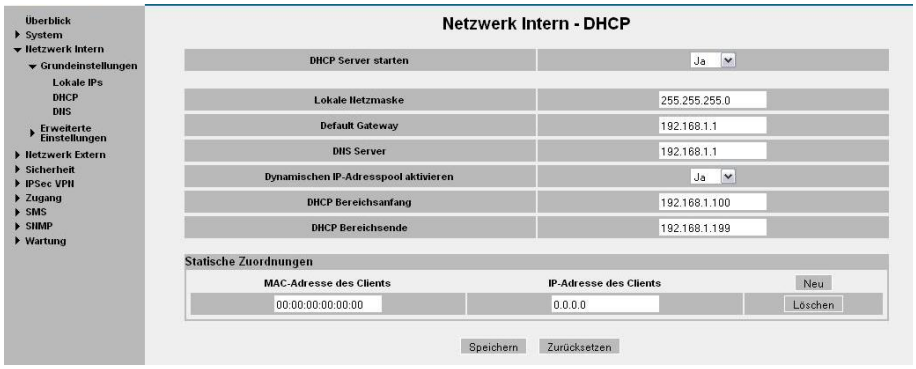
Sie können weitere Adressen festlegen, unter denen das TAINY xMOD von lokalen Applikationen erreicht werden kann. Dies ist dann hilfreich, wenn z.B. das lokale Netz in Subnetze unterteilt wird. Dann können mehrere lokale Applikationen aus verschiedenen Subnetzen das TAINY xMOD unter unterschiedlichen Adressen erreichen.

Neu Fügt weitere IP-Adressen und Netzmasken hinzu, die Sie wiederum ändern können.

Löschen Entfernt die jeweilige IP-Adresse und Netzmaske. Der erste Eintrag kann nicht gelöscht werden.

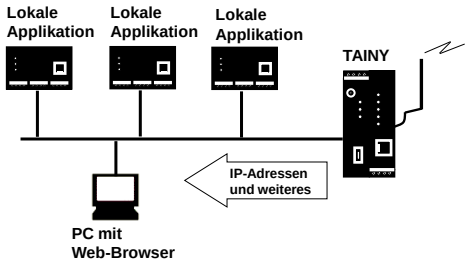
4.2 DHCP-Server zum lokalen Netz

Netzwerk Intern > Grundeinstellungen > DHCP



DHCP Funktion

Das TAINY xMOD beinhaltet einen DHCP-Server (DHCP = Dynamic Host Configuration Protokoll). Ist der DHCP-Server eingeschaltet, weist er den Applikationen, die an der lokalen Schnittstelle des TAINY xMOD angeschlossen sind, automatisch die IP-Adressen, Netzmasken, das Gateway und den DNS-Server zu. Dazu muss bei den lokalen Applikationen das automatische Beziehen der IP-Adresse und der Konfigurationsparameter per DHCP aktiviert sein.



DHCP-Server starten

Mit *DHCP-Server starten – Ja* schalten Sie den DHCP-Server des TAINY xMOD ein, mit *Nein* wird er ausgeschaltet.

Lokale Netzwerkmaske

Tragen Sie hier die lokale Netzmaske ein, die den lokalen Applikationen zugewiesen werden soll.

Default Gateway

Tragen Sie hier das Default Gateway ein, das den lokalen Applikationen zugewiesen werden soll.

DNS-Server

Tragen Sie hier den DNS-Server ein, der den lokalen Applikationen zugewiesen werden soll.

Dynamischen IP-Adresspool aktivieren

Bei *Ja* werden die IP-Adressen, die der DHCP-Server des TAINY xMOD vergibt aus einem dynamischen Adresspool entnommen,

Bei *Nein* müssen die IP-Adressen unter *Statische Zuordnung* den MAC-Adressen der lokalen Applikationen zugeordnet werden.

DHCP Bereichsanfang

Gibt die erste Adresse des dynamischen Adresspools an.

DHCP Bereichsende

Gibt die letzte Adresse des dynamischen Adresspools an.

Statische Zuordnung

Bei Statischer Zuordnung der IP-Adressen, können Sie den MAC-Adressen lokaler Applikationen korrespondierende IP-Adressen fest zuweisen.

Fordert eine lokale Applikation per DHCP die Zuweisung einer IP-Adresse, übermittelt die Applikation bei der DHCP-Anfrage seine MAC-Adresse. Ist dieser MAC-Adresse eine IP-Adresse statisch zugeordnet, weist TAINY xMOD der Applikation die korrespondierende IP-Adresse zu.

MAC-Adresse des Clients –

MAC-Adresse der anfragenden lokalen Applikation

IP-Adresse des Clients –

zugeordnete IP-Adresse

Werkseinstellung

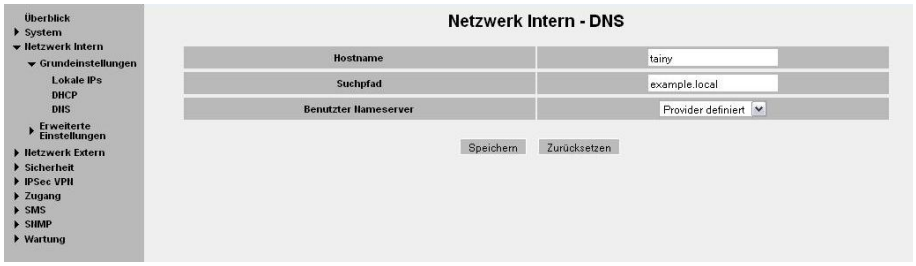
Werkseitig hat das TAINY xMOD folgende Einstellungen:

DHCP-Server starten	**Nein**
Lokale Netzwerkmaske	**255.255.255.0**
Default Gateway	**192.168.1.1**
DNS-Server	**192.168.1.1**
Dynamischen IP-Adresspool aktivieren	**Nein**
DHCP Bereichsanfang	**192.168.1.100**

DHCP Bereichsende **192.168.1.199**

4.3 DNS zum lokalen Netz

Netzwerk Intern > Grundeinstellungen > DNS

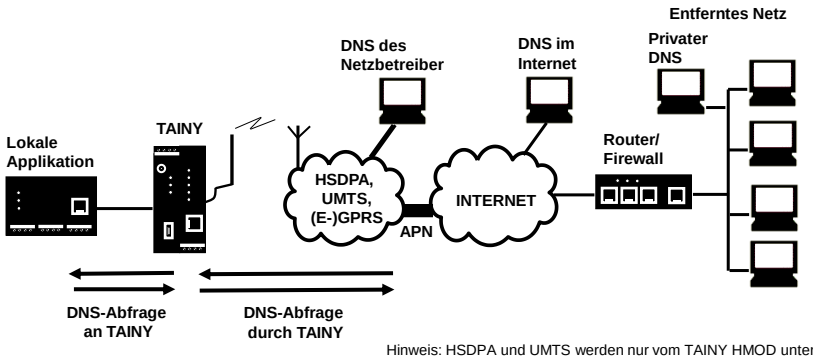


DNS Funktion

Das TAINY xMOD stellt dem lokalen Netz einen Domain Name Server (DNS) bereit.

Tragen Sie in Ihrer lokalen Applikation die IP-Adresse des TAINY xMOD als Domain Name Server (DNS) ein, dann beantwortet das TAINY xMOD die DNS-Abfragen aus seinem Cache. Kennt es zu einer Domain-Adresse nicht die dazugehörige IP-Adresse, leitet das TAINY xMOD diese Abfragen weiter an einen externen Domain Name Server (DNS).

Die Zeitspanne, in der das TAINY xMOD eine Domain-Adresse im Cache behält, ist abhängig vom adressierten Host. Die DNS-Abfragen an einen externen Domain Name Server, liefern außer der IP-Adresse auch die Lebensdauer dieser Information zurück.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Als externe Domain Name Server (DNS) können Server des Netzbetreibers, Server im Internet oder Server im privaten externen Netz verwendet werden.

Benutzter Nameserver

Wählen Sie aus, bei welchen Domain Name Server (DNS) das TAINY xMOD nachfragen soll:

Provider definiert	Beim Verbindungsaufbau zum Datenfunkdienst (HSDPA/UMTS/EGPRS/GPRS) übermittelt der Netzbetreiber automatisch eine oder mehrere DNS-Adressen.
Benutzer definiert	Sie wählen als Anwender Ihre(n) bevorzugten DNS aus. Die DNS können mit dem Internet verbunden sein oder es kann ein privater DNS in Ihrem Netz sein.

Benutzer definierte Nameserver

Wenn Sie die Option *Benutzer definiert* gewählt haben, dann geben Sie bitte die IP-Adresse des ausgewählten DNS als *Server IP-Adresse* ein.

Mit *Neu* können Sie weitere DNS hinzufügen.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Benutzter Nameserver **Provider definiert**

Benutzer definierte Nameserver	**-**
bei neuem Eintrag	**0.0.0.0**

4.4 Lokaler Hostname

Netzwerk Intern > Grundeinstellungen > DNS

Das TAINY xMOD kann aus dem lokalen Netz, auch über einen Hostnamen adressiert werden. Legen Sie dazu einen Hostnamen fest, z.B. *myTAINY*.

Das TAINY xMOD kann dann zum Beispiel von einem Web-Browser als *myTAINY* aufgerufen werden.

Hinweis

Das Sicherheitskonzept des TAINY xMOD macht es erforderlich, dass für jede lokale Applikation, die diese Hostname-Funktion nutzen soll, eine ausgehende Firewall-Regel erstellt wird. Siehe Kapitel 6.1.

Wenn Sie kein DHCP, siehe Kapitel 4.2 verwenden, müssen im TAINY xMOD und in den lokalen Applikationen manuell identische Suchpfade eingetragen werden. Wenn Sie DHCP verwenden, erhalten die lokale Applikationen den im TAINY xMOD eingetragenen Suchpfad per DHCP.

Werkseinstellung

Werkseitig hat das TAINY HMOD folgende Einstellungen:

NUR TAINY HMOD

Suchpfad	**example.local**
Hostname	**tainy**

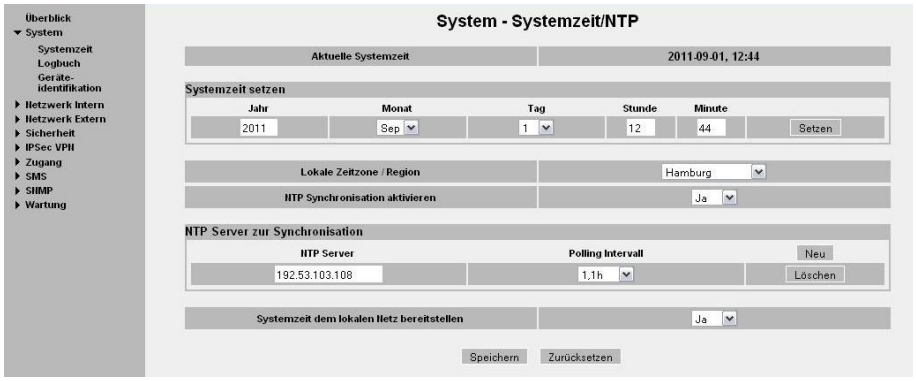
NUR TAINY EMOD

Werkseitig hat das TAINY EMOD folgende Einstellungen:

Suchpfad	**example.local**
Hostname	**tainy**

4.5 Systemzeit / NTP

System > Systemzeit



Systemzeit setzen

An dieser Stelle setzen Sie die Systemzeit für das TAINY xMOD. Diese Systemzeit wird:

- als Zeitstempel für alle Logbuch-Einträge benutzt und
- dient als Zeitbasis für alle zeitgesteuerten Funktionen.

Wählen Sie Jahr, Monat und Tag sowie Stunde und Minute.

NTP Synchronisation aktivieren

Das TAINY xMOD kann die Systemzeit auch über NTP (= *Network Time Protokoll*) von einem Zeitserver beziehen. Im Internet gibt es eine Reihe von Zeitservern von denen die aktuelle Uhrzeit sehr präzise mittels NTP bezogen werden kann.

Lokale Zeitzone / Region

Die NTP-Zeitserver übermitteln die UTC (= *Universal Time Coordinated*), d.h. die koordinierte Weltzeit. Wählen Sie eine Stadt in der Nähe des Standortes aus, an dem das TAINY xMOD arbeiten soll und legen Sie so die Zeitzone fest. Dann wird die Uhrzeit dieser Zeitzone als Systemzeit verwendet.

NTP-Server

Klicken Sie auf *Neu*, um einen NTP-Server hinzuzufügen und geben Sie die IP-Adresse eines solchen NTP-Servers ein oder verwenden Sie den ab Werk voreingestellten NTP-Server. Sie können parallel mehrere NTP-Server angeben.

Die Eingabe der NTP-Adresse als Hostname (z.B. timeserver.org) ist nicht möglich.

Polling Intervall

Die Zeitsynchronisation erfolgt zyklisch. Das Intervall, in dem die Synchronisation stattfindet, bestimmt das TAINY xMOD automatisch. Spätestens nach 36 Stunden findet erneut eine Synchronisation statt. Das Polling Intervall legt fest, wie lange das TAINY xMOD mindestens bis zur nächsten Synchronisation wartet.

Hinweis

Die Synchronisation der Systemzeit über NTP verursacht ein zusätzliches Datenaufkommen auf der Datenfunk-Verbindung. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 120 kByte im Monat und mehr betragen. Je nach Teilnehmervertrag mit dem GSM-Netzbetreiber sind damit erhöhte Kosten verbunden.

Systemzeit dem lokalen Netz bereitstellen

Das TAINY xMOD kann selber als NTP-Zeitserver für die Applikationen dienen, die an seiner lokalen Netzwerkschnittstelle angeschlossen sind. Zur Aktivierung dieser Funktion wählen Sie *Ja*.

Der NTP-Zeitserver im TAINY xMOD ist über die eingestellte lokale IP-Adresse des TAINY xMOD erreichbar, siehe Kapitel 4.1.

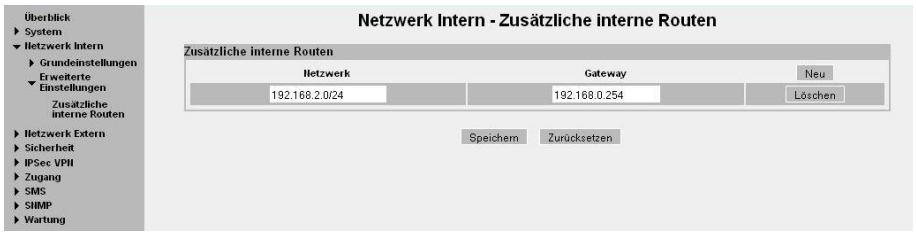
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Lokale Zeitzone	**UTC**
NTP Synchronisation aktivieren	**Nein**
NTP-Server	**192.53.103.108**
Polling Intervall	**1.1 Stunden**
Systemzeit dem lokalen Netz bereitstellen	**Nein**

4.6 Zusätzliche interne Routen

Netzwerk Intern > Erweiterte Einstellungen > Zusätzliche interne Routen



Funktion

Teilt sich das lokale Netz in Subnetze auf, können Sie zusätzliche Routen definieren.

Siehe auch Kapitel 12.

Wollen Sie eine weitere Route zu einem Subnetz festlegen, klicken Sie *Neu*.
Geben Sie folgendes an:
- die IP-Adresse des Subnetzes (Netzwerkes), ferner
- die IP-Adresse des Gateways, über das das Subnetz angeschlossen ist.

Sie können beliebig viele interne Routen festlegen.

Wollen Sie eine interne Route löschen, klicken Sie *Löschen*.

Werkseinstellung

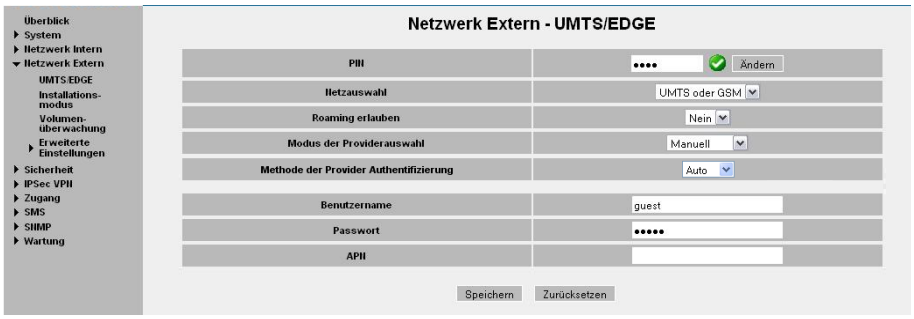
Werkseitig hat das TAINY xMOD folgende Einstellungen:

Zusätzliche interne Routen	**-**
Vorgabe für neue Routen:	
Netzwerk:	**192.168.2.0/24**
Gateway:	**192.168.0.254**

5 Externe Schnittstelle

5.1 Netzauswahl und Zugangsparameter für UMTS bzw. EGPRS und GPRS

Netzwerk Extern > UMTS/EDGE

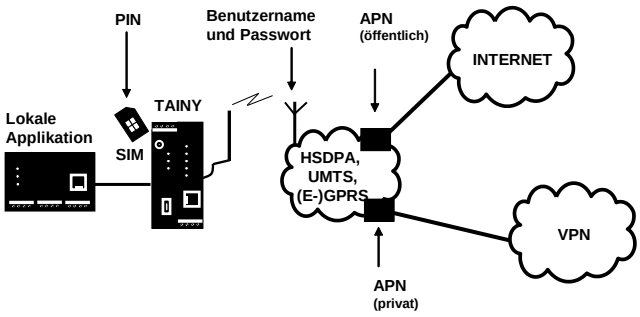


Funktion

Das TAINY HMOD verwendet als Datenfunkdienst HSDPA, UMTS data, EGPRS oder GPRS zur Kommunikation mit dem externen Netz. Auszuwählen ist der Typ des Mobilfunknetzes (UMTS oder GSM).

Das TAINY EMOD verwendet als Datenfunkdienst EGPRS oder GPRS. Für den Zugang zu diesen IP-Mobillfunkdiensten und zum grundlegenden Funknetz sind Zugangsparameter erforderlich, die Sie von Ihrem Mobilfunkbetreiber erhalten.

Die PIN schützt die SIM-Karte vor unbefugter Benutzung. Benutzername und Passwort schützen den Zugang zum Datenfunkdienst und der APN (Access Point Name) definiert den Übergang vom Datenfunkdienst zu weiteren verbundenen IP-Netzen, z.B. einen öffentlichen APN zum Internet oder einen privaten APN zu einem Virtual Private Network (VPN).



Netzauswahl

NUR TAINY HMOD

Das TAINY HMOD kann sich wahlweise mit UMTS- oder GSM-Mobilfunknetzen verbinden.

- UMTS (mit den Diensten UMTS data und HSDPA)
- GSM (mit den Diensten EGPRS, GPRS und CSD)

Bei der Einstellung *UMTS oder GSM* wählt das TAINY HMOD nach Verfügbarkeit vorrangig ein UMTS-Netz aus. Falls nicht erreichbar wird ein GSM-Netz verwendet.

Bei der Einstellung *Nur UMTS* wählt das TAINY HMOD in jedem Fall ein UMTS-Netz aus.

Bei der Einstellung *Nur GSM* wählt das TAINY HMOD in jedem Fall ein GSM-Netz aus.

Roaming erlauben

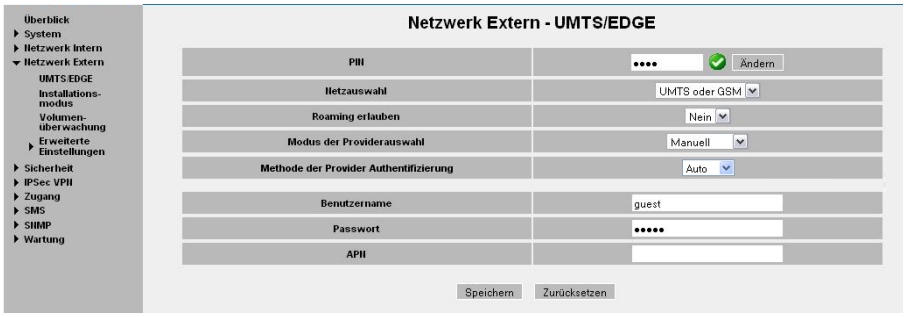
Wählen Sie *Nein*, wenn sich das TAINY xMOD ausschliesslich in das Heimatnetz, d.h. in das Mobilfunknetz einbuchen soll, dessen SIM-Karte eingelegt ist.

Wählen Sie *Ja*, wenn sich das TAINY xMOD auch in die Partnernetze des Heimatnetzes einbuchen darf, sollte das Heimatnetz nicht oder schlechter erreichbar sein.

Warnung

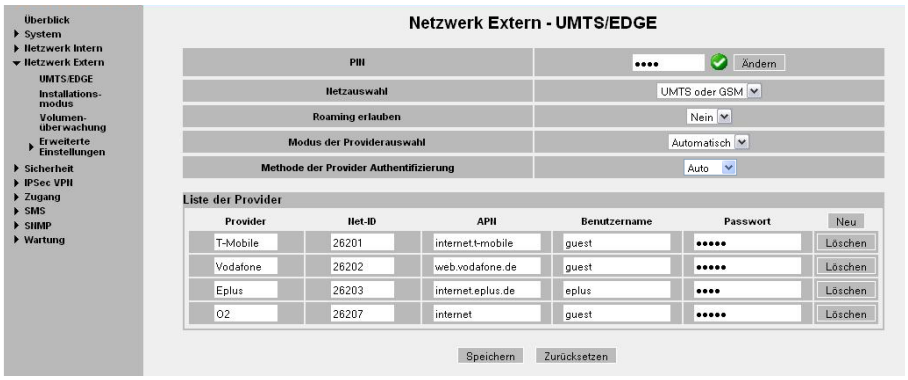
Bucht sich das TAINY xMOD in ein Partnernetz ein (Roaming) kann dies zu erheblichen Mehrkosten führen.

Modus der Providerauswahl - Manuell



Ist als Modus der Providerauswahl Manuell ausgewählt, geben Sie Benutzername, Passwort und APN für die UMTS- bzw. GSM-Dienste händisch ein.

Modus der Providerauswahl - Automatisch



Ist als Modus der Providerauswahl Automatisch ausgewählt, werden die Zugangsdaten für den UMTS- oder GSM-Dienste automatisch anhand der Net-ID der SIM-Karte aus der Liste der Provider ausgewählt. Es können mehrere Einträge in der Liste angelegt werden. Die Anzahl ist nicht beschränkt, mehr als 10 Einträge sollten aber vermieden werden.

Mit *Neu* kann ein neuer Eintrag hinzugefügt werden. Mit *Löschen* werden Einträge entfernt.

PIN

Geben Sie hier die PIN zu Ihrer SIM-Karte ein. Sie erhalten die PIN von Ihrem Netzbetreiber.

Das TAINY xMOD arbeitet auch mit PIN-losen SIM-Karten, in diesem Fall geben Sie bitte ***NONE*** ein. Das Eingabefeld bleibt in diesem Fall leer.

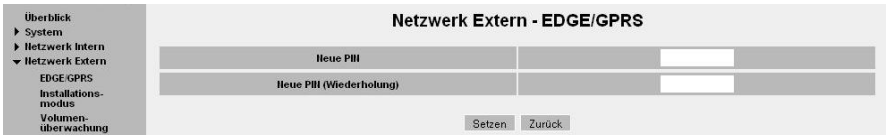
Hinweis

Das Eingabefeld der PIN wird nach dem Speichern rot umrandet, wenn keine Eingabe erfolgt.

PIN ändern

Um die PIN auf der SIM-Karte zu ändern, betätigen Sie die Schaltfläche *Ändern*.

Es öffnet sich ein Untermenü.



Neue PIN

Geben Sie hier die neue PIN ein.

Neue PIN (Wiederholung)

Geben Sie hier die neue PIN zur Bestätigung nochmals ein.

Hinweis

Ist die PIN-Abfrage bei der eingelegten SIM-Karte deaktiviert (Pin-lose Karte), kann die PIN nicht aktiviert bzw. geändert werden.

Provider (nur bei Providerauswahl Automatisch)

Geben Sie hier als Freitext eine Bezeichnung für den UMTS- oder GPRS-Dienst an, beispielsweise den Namen des Provider (z.B. Vodafone, Eplus, mein GPRS-Zugang).

Net-ID (nur bei Providerauswahl Automatisch)

Geben Sie hier die Identifikations-Nummer des Netzbetreibers (Provider) ein, auf die sich die UMTS- oder GPRS-Zugangsdaten in der gleichen Zeile der Liste der Provider beziehen.

Jeder GSM/GPRS-Netzbetreiber hat eine weltweit einmalig vergebene Identifikations-Nummer. Diese ist auf der SIM-Karte gespeichert. Das TAINY xMOD liest diese Net-ID von der SIM-Karte und wählt die entsprechenden UMTS- oder GPRS-Zugangsdaten aus der Liste der Provider.

Sie finden die NET-ID auf unserer Web-Seite www.neuhaus.de, in den Unterlagen Ihres GSM/GPRS-Netzbetreibers, auf seiner Internetseite oder erfragen ihn bei dessen Hotline (Stichwort MCC/MNC).

Benutzername

Geben Sie hier den Benutzername für den Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld *gast* ein.

Passwort

Geben Sie hier das Passwort für den Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) ein. Einige Mobilfunkbetreiber verzichten auf die Zugangskontrolle durch Benutzername und/oder Passwort. In diesem Fall tragen Sie in das jeweilige Feld *gast* ein.

APN

Geben Sie hier den Namen des Übergangs vom Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) zu weiteren Netzen ein.

Sie finden den APN in den Unterlagen Ihres Mobilfunkbetreibers, auf seiner Internetseite oder erfragen ihn bei dessen Hotline.

Methode der Provider Authentifizierung

Für die Anmeldung am Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) werden zwei verschiedene Verfahren (PAP und CHAP) genutzt. In der Regel erfolgt die Auswahl des Verfahrens automatisch. Soll ein bestimmtes Verfahren benutzt werden, so kann die Auswahl manuell erfolgen. Wählen Sie aus zwischen Auto, PAP oder CHAP.

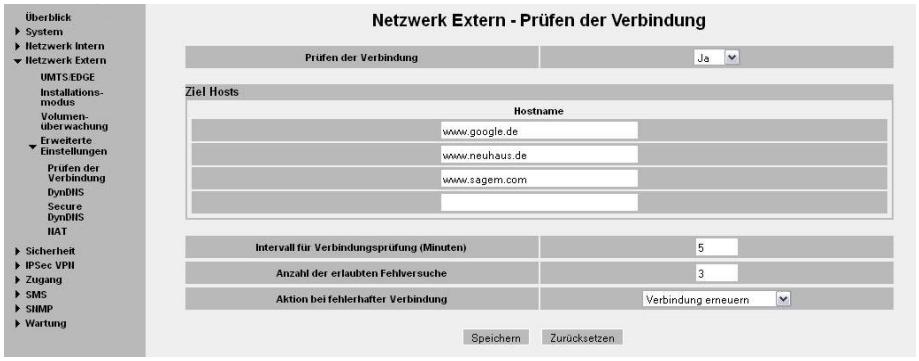
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Nur TAINY HMOD-V2-IO	Netzauswahl	**UMTS oder GSM**
	Modus der Providerauswahl	**Automatisch**
	Roaming	**Nein**
	PIN	**NONE**
Modus der Providerauswahl - Manuell	Benutzername	**guest**
	Passwort	**guest**
	APN	**NONE**
Modus der Providerauswahl - Automatisch	1. Provider	**T-Mobile**
	Net-ID	**26201**
	Benutzername	**guest**
	Passwort	**guest**
	APN	**internet.t-mobile**
	2. Provider	**Vodafone**
	Net-ID	**26202**
	Benutzername	**guest**
	Passwort	**guest**
	APN	**web.vodafone.de**
	3. Provider	**Eplus**
	Net-ID	**26203**
	Benutzername	**guest**
	Passwort	**guest**
	APN	**internet.eplus.de**
	4. Provider	**O2**
	Net-ID	**26207**
	Benutzername	**guest**
	Passwort	**guest**
	APN	**internet**
	n. Provider	**NONE**
	Net-ID	**NONE**
	Benutzername	**guest**
	Passwort	**guest**
	APN	**NONE**
	Methode der Provider Authentifizierung	**Auto**

5.2 Überwachung der Datenfunkdienst-Verbindung

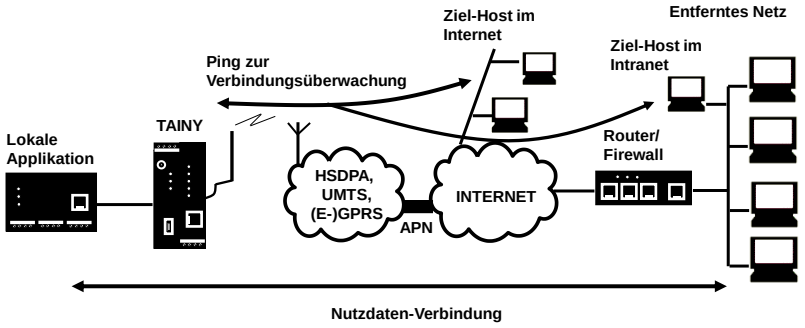
Netzwerk Extern > Erweiterte Einstellungen > Prüfen der Verbindung



Funktion

Mit der Funktion *Prüfen der Verbindung* überprüft das TAINY xMOD seine Verbindung zum Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) und zu den angeschlossenen externen Netzen, wie z.B. dem Internet oder einem Intranet. Dazu sendet das TAINY xMOD in regelmäßigen Zeitabständen, Ping-Pakete (ICMP) an bis zu vier Gegenstellen (Ziel Hosts). Dies geschieht unabhängig von den Nutzdaten-Verbindungen. Erhält das TAINY xMOD auf einen solchen Ping mindestens von einer der adressierten Gegenstellen eine Antwort, ist das TAINY xMOD noch mit dem Datenfunkdient (HSDPA, UMTS, EGPRS oder GPRS) verbunden und betriebsbereit.

Einige *Netzbetreiber* unterbrechen Verbindungen bei Inaktivität. Dem wird durch die Funktion *Prüfen der Verbindung* ebenfalls vorgebeugt.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Warnung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über den Datenfunkdienst (HSDPA, UMTS, EGPPS oder GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 2,5 MByte im Monat (Ping an IP-Adresse) bzw. 6 Mbyte im Monat (Ping an Hostnamen) und mehr betragen. Dies kann zu erhöhten Kosten führen.

Prüfen der Verbindung

Bei *Ja* ist die Funktion eingeschaltet.

Zielhosts - Hostname

Wählen Sie bis zu vier Gegenstellen aus, die das TAINY xMOD anpingen kann. Die Gegenstellen müssen ständig erreichbar sein und Ping beantworten.

Hinweis

Vergewissern Sie sich, dass sich die ausgewählten Gegenstellen nicht „belästigt“ fühlen.

Intervall für Verbindungsprüfung (Minuten)

Legt das Intervall fest mit dem die Ping-Pakete der Verbindungsüberwachung vom TAINY xMOD versendet werden. Die Angabe erfolgt in Minuten.

Anzahl der erlaubten Fehlversuche	Legt fest, wie oft es vorkommen darf, dass alle Ping-Pakete eines Intervalls nicht beantwortet werden, d.h. dass bei vier angepingten Gegenstellen keine antwortet, bevor die festgelegte Aktion durchgeführt wird.	
Aktion bei fehlerhafter Verbindung	*Verbindung erneuern*	Das TAINY xMOD stellt erneut die Verbindung zum Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) her, falls die gesendeten Ping-Pakete nicht beantwortet wurden.
	Neustart des TAINY xMOD	Das TAINY xMOD führt einen Neustart durch, falls die gesendeten Ping-Pakete nicht beantwortet wurden.

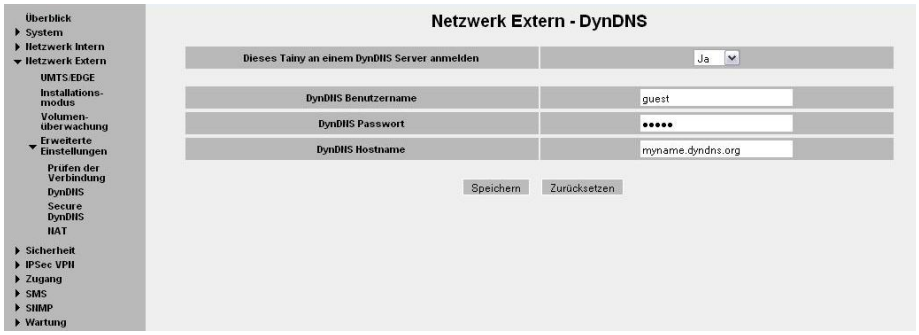
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

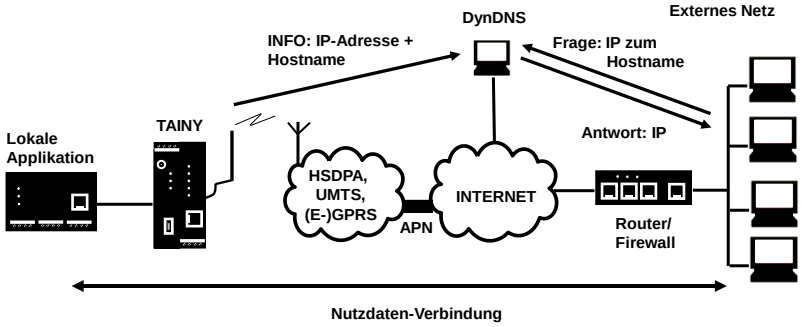
Prüfen der Verbindung	**Nein (Ausgeschaltet)**
Hostname	**-**
Intervall für Verbindungsprüfung	**5 (Minuten)**
Anzahl der erlaubten Fehlversuche	**3 (Fehlversuche)**
Aktion bei fehlerhafter Verbindung	**Verbindung erneuern**

5.3 Hostname durch DynDNS

Netzwerk Extern > Erweiterte Einstellungen > DynDNS



Funktion	Dynamische Domain Name Server (DynDNS) ermöglichen es Applikationen im Internet, unter einem Hostnamen (z.B. myHost.org) erreichbar zu sein, auch wenn diese Applikationen keine feste IP-Adresse haben und der Hostname nicht registriert ist. Wenn Sie das TAINY xMOD bei einem DynDNS-Dienst anmelden, können Sie das TAINY xMOD aus dem externen Netz auch unter einem Hostnamen erreichen, z.B. myTainy.dyndns.org. Mehr Informationen zu DynDNS finden Sie im Kapitel 12.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Dieses TAINY an einem DynDNS-Server anmelden	Wählen Sie *Ja,* wenn Sie einen DynDNS-Dienst verwenden wollen.
DynDNS-Anbieter	Das TAINY xMOD ist kompatibel zu dyndns.org.
DynDNS Benutzername / Passwort	Geben Sie hier den Benutzernamen und das Passwort ein, das Sie zur Nutzung des DynDNS-Service berechtigt. Ihr DynDNS-Anbieter teilt Ihnen diese Angaben mit.
DynDNS Hostname	Geben Sie hier den Hostnamen ein, den Sie für das TAINY xMOD mit Ihrem DynDNS-Anbieter vereinbart haben, z.B. myTAINY.dyndns.org.

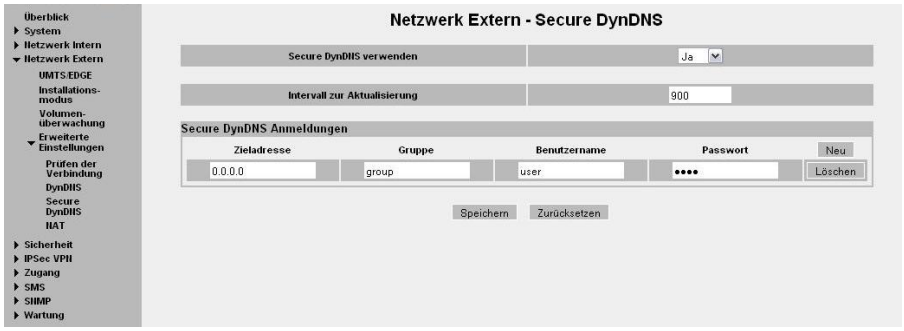
Werkseinstellung

Werkseitig hat TAINY xMOD folgende Einstellungen:

Das TAINY an einem DynDNS-Server anmelden	**Nein (Ausgeschaltet)**
DynDNS Benutzername	**guest**
DynDNS Passwort	**guest**
DynDNS Hostname	**myname.dyndns.org**

5.4 Secure DynDNS

Netzwerk Extern > Erweiterte Einstellungen > Secure DynDNS



Funktion	Bei aktivierter Secure DynDNS Funktion übermittelt das TAINY xMOD seine vom Datenfunkdienst zugewiesene externe IP-Adresse per gesichertem https-Protokoll an einen einstellbaren Zielserver. Das Verfahren ist vergleichbar mit dem DynDNS-Dienst und erfordert einen entsprechenden Zugang auf der Serverseite.
SecureDynDNS verwenden	Wählen Sie *Ja*, wenn Sie den Siemens Remote Service verwenden wollen. Mit *Neu* können Sie weitere Zielserver hinzufügen, mit *Löschen* bestehende Einträge entfernen.

Intervall zur Aktualisierung	Geben Sie hier das Intervall in Sekunden an, mit dem die zugewiesene IP-Adresse des TAINY xMOD an den eingestellten Zielserver übertragen werden soll.
SecureDynDNS Anmeldungen	Geben Sie hier die Zieladresse und die Zugangsdaten einem oder mehren Zielservern an:
	Zieladresse
	Geben Sie hier die IP-Adresse des Zielservers an.
	Gruppe
	Geben Sie hier die Gruppen-Information ein.
	Benutzername
	Geben Sie hier den Benutzernamen für den Zugang am Zielserver ein.
	Passwort
	Geben Sie hier das Passwort für den Zugang am Zielserver ein.

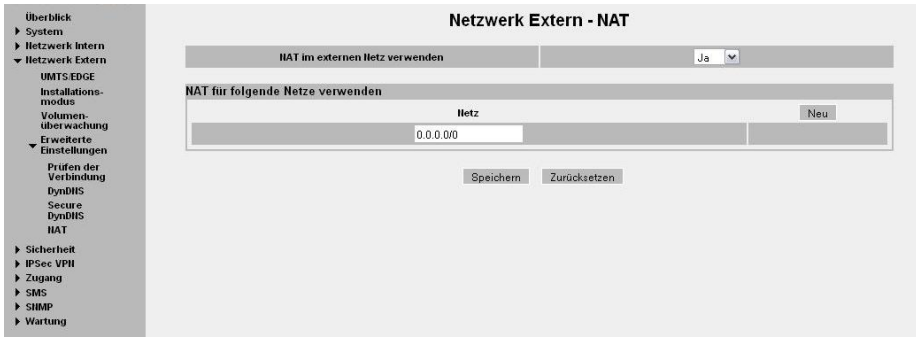
Werkseinstellung

Werkseitig hat TAINY xMOD folgende Einstellungen:

Secure DynDNS verwenden	**Nein (Ausgeschaltet)**
Intervall zur Aktualisierung	**900 Sekunden**
Zieladresse	**0.0.0.0**
Gruppe	**group**
Benutzername	**user**
Passwort	**pass**

5.5 NAT – Network Address Translation

Netzwerk Extern > Erweiterte Einstellungen > NAT



Funktion	Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf und ermöglicht, Regeln zu setzen oder zu löschen.
	Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.
	Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x benutzt wird oder weil die interne Netzstruktur verborgen werden soll.
	Dieses Verfahren wird auch *IP-Masquerading* genannt.
NAT im externen Netz verwenden	Wählen Sie *Ja*, um die NAT Funktion zum externen Netz zu aktivieren.

NAT für folgende Netze verwenden	Geben Sie die Netzwerke an, für die NAT genutzt werden soll. Die Angabe erfolgt als Adressbereich. Verwenden Sie die CIDR Syntax *Neu* – Netzwerk hinzufügen *Löschen* – Netzwerk löschen

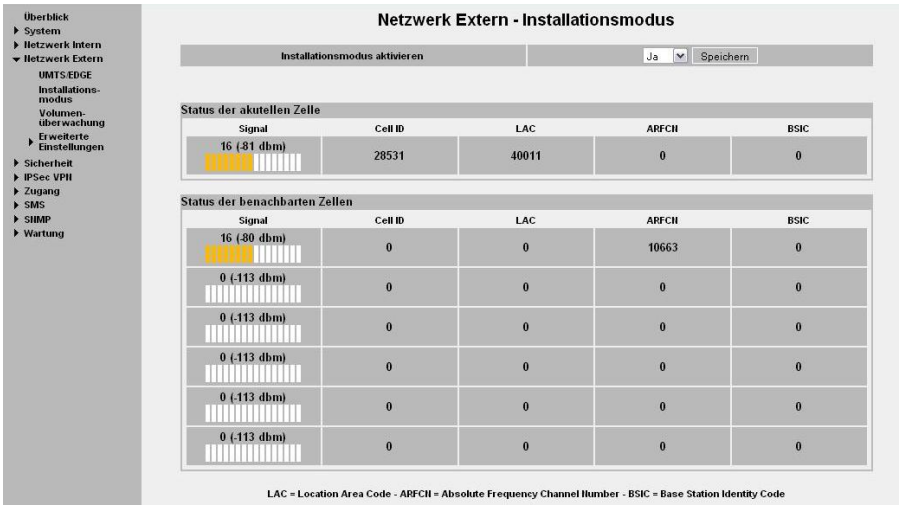
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

NAT für folgende Netze verwenden	**Ja (Eingeschaltet)**
Netzwerk	**0.0.0.0/0**.

5.6 Installationsmodus

Netzwerk Extern - Installationsmodus



Der Installatonsmodus unterstützt das Positionieren der Antenne und gibt Infomationen über die Funkzellen in der Umgebung. Ist der Installationsmodus aktiviert, werden alle drei Sekunden die gemessenen Signalstärken und weitere Kenndaten der Funkzellen in der Umgebung aktualisiert

Ebenso wird im Installationsmodus die Anzeige der Signalleuchte Q (Quality) alle 3 Sekunden aktualisiert. Im Nomalbetrieb mit aufgebauter Verbindung erfolgt die Abfrage dieser Daten im Abstand von 60 Sekunden.

Die Position der Antenne sollte solange verändert werden, bis das angezeigte Signal der aktuellen Zelle ein Maximum erreicht hat.

Installationsmodus aktivieren	Wählen Sie *Ja*, um den Installationsmodus einzuschalten. Wählen Sie *Nein*, um den Installationsmodus auszuschalten und zum Normabetrieb zurückzukehren.

Achtung

Im Installationsmodus sind alle Nutzverbindungen zum externen Netz unterbrochen. Ein normaler Wirkbetrieb ist im Installationsmodus nicht möglich.

Status der aktuellen Zelle	Zeigt die Kenndaten der Funkzelle an, mit der das TAINY xMOD aktuell verbunden ist.
Status der benachbarten Zellen	Zeigt die Kenndaten benachbarter Funkzellen an, von denen das TAINY xMOD Signale empfängt.
Signal	Anzeige der Qualität / Feldstärke mit der das Signal der Funkzelle empfangen wird. Angegeben wird der CSQ-Wert und umgerechnet als RSSI-Wert [dBm].

Cell-ID	Gibt die Kennung (Cell-ID) der Funkzelle an.
LAC	Gibt die Kennung (LAC) des aus mehreren Basisstationen / Funkzellen bestehenden Netzabschnittes in der Umgebung des TAINY xMOD an.
ARFCN	Gibt die Nummer (ARFCN) des Funkkanal an, auf dem die Funkzelle sendet.
BSIC	Gibt die Kennung (BSIC) der Basisstation an, zu der die Funkzelle gehört.

5.7 Volumenüberwachung

Netzwerk Extern – Volumen-Überwachung

Überschreitet die Menge der vom TAINY xMOD gesendeten und empfangenen Daten das mit dem Mobilfunkbetreiber vereinbarte Datenvolumen, kann dies zu erheblichen Mehrkosten führen.

Daher kann es nützlich sein, wenn das TAINY xMOD das genutzte Datenvolumen ständig überwacht und bei drohender Überschreitung eines einstellbaren Grenzwertes eine Warnung versendet.

Volumenüberwachung aktivieren	Wählen Sie *Ja*, um die Volumenüberwachung einzuschalten. Wählen Sie *Nein*, um die Volumenüberwachung auszuschalten.
Übertragene Bytes seit Monatsbeginn	Zeigt die Anzahl der gesendeten und empfangenen Bytes seit Monatsbeginn an.

Hinweis

Setzen Sie manuell die Systemzeit des TAINY xMOD oder aktivieren Sie die NTP-Synchronisation, siehe Kapitel 4.5.

Zurücksetzen	Betätigen Sie die Schaltfläche, wenn Sie den Zähler für die gesendeten und empfangenen Bytes auf 0 zurücksetzen wollen. Zum Monatswechsel geschieht dies automatisch.
Maximales Datenvolumen in Bytes pro Monat	Tragen Sie hier den Grenzwert für das monatliche Datenvolumen in Bytes ein.
Warn-SMS bei Volumen-überschreitung (80%)	Wählen Sie *Ja*, wenn das TAINY xMOD bei Erreichen von 80% des maximalen Datenvolumens eine SMS mit Warnmeldung an die angegebene Rufnummer versenden soll.
Alarm-SMS bei Volumen-überschreitung (100%)	Wählen Sie *Ja*, wenn das TAINY xMOD bei Erreichen des maximalen Datenvolumens eine SMS mit Alarmmeldung an die angegebene Rufnummer versenden soll.
Rufnummer	Geben Sie hier die Mobilfunkrufnummer an, an die die SMS mit Alarm- oder Warnmeldung gesendet werden soll.
Text	Geben Sie hier den Text der Alarm- bzw Warn-SMS ein.

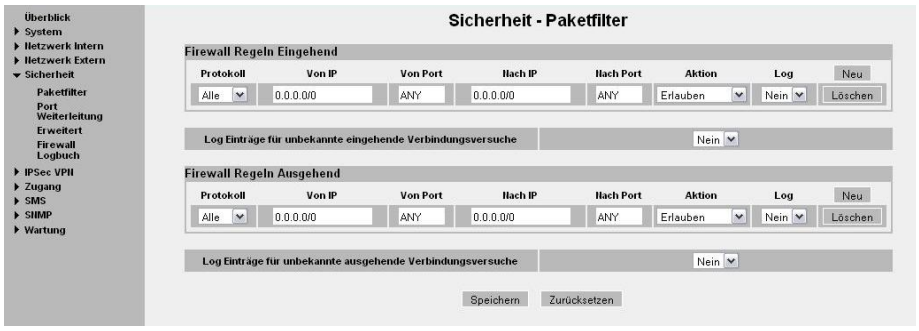
Hinweis

Das ermittelte Datenvolumen dient nur als Anhaltspunkt und kann von der Abrechnung des GSM-Netzbetreibers abweichen.

6 Sicherheitsfunktionen

6.1 Paketfilter

Sicherheit > Paketfilter



Funktion

Das TAINY xMOD beinhaltet eine Stateful Inspection Firewall.

Stateful Inspection Firewall ist eine Methode zur Paketfilterung. Paketfilter lassen IP-Pakete nur dann passieren, wenn dies zuvor durch Firewall-Regeln definiert wurde. In der Firewall-Regel wird folgendes festgelegt,

- welches Protokoll (TCP, UDP, ICMP) passieren darf,
- die erlaubte Quelle der IP-Pakete (Von IP / Von Port)
- das erlaubte Ziel der IP-Pakete (Nach IP / Nach Port)

Gleichfalls wird hier festgelegt, wie mit IP-Pakete verfahren wird, die nicht passieren dürfen (verwerfen, zurückweisen).

Bei einem einfachen Paketfilter müssen immer zwei Firewall-Regeln für eine Verbindung angelegt werden:

- Eine Regel für die Anfragerichtung von der Quelle zum Ziel und
- eine zweite Regel für die Antwortrichtung vom Ziel zur Quelle.

Anders beim TAINY xMOD mit Stateful Inspection Firewall. Hier wird nur für die Anfragerichtung von der Quelle zum Ziel eine Firewall-Regel angelegt. Die Firewall-Regel für die Antwortrichtung vom Ziel zur Quelle ergibt sich aus der Analyse der zuvor gesendeten Daten. Die Firewall-Regel für die Antworten wird nach Erhalt der Antworten bzw. nach Ablauf einer kurzen Zeitspanne wieder geschlossen. Antworten dürfen also nur passieren, wenn es zuvor eine Anfrage gab. So kann die Antwortregel nicht für unbefugte Zugriffe benutzt werden. Besondere Verfahren ermöglichen zudem, dass auch UDP- und ICMP-Daten passieren können, obwohl diese Daten zuvor nicht angefordert wurden.

Firewall-Regeln Eingehend

Mit den Firewall-Regeln Eingehend wird festgelegt, wie mit IP-Paketen zu verfahren ist, die über den Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) aus externen Netzen (z.B. Internet) empfangen werden. Quelle ist der Absender dieser IP-Pakete. Ziel sind die lokalen Applikationen am TAINY xMOD.

Entsprechend der Werkseinstellung ist zunächst keine eingehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Löschen Entfernt angelegte Firewall-Regeln wieder.

Protokoll Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen *TCP, UDP, ICMP*. Wenn Sie *Alle* wählen, gilt die Regel für alle drei Protokolle.

Hinweis

Wird für Protokoll *Alle* gewählt ist eine Portzuordnung nicht wirksam.

Von IP Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

Von Port Tragen Sie den Port (z.B. 80) oder Portbereich (z.B. 8080:9090) ein, von dem die externe Gegenstelle IP-Pakete senden darf.

(wird nur ausgewertet bei den Protokollen TCP und UDP)

Nach IP Tragen Sie ein, an welche IP-Adresse im lokalen Netz IP-Pakete gesendet werden dürfen. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im lokalen Netz an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

Nach Port Tragen Sie den Port (z.B. 80) oder Portbereich (z.B. 8080:9090) ein, an den die externe Gegenstelle IP-Pakete senden darf.

Aktion Wählen Sie aus, wie mit eintreffenden IP-Paketen zu verfahren ist:

Erlauben – Die Datenpakete dürfen passieren,

Zurückweisen – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung,

Verwerfen – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.

Firewall-Regeln Ausgehend

Mit den Firewall-Regeln Ausgehend wird festgelegt, wie mit IP-Paketen zu verfahren ist, die vom lokaken Netz empfangen werden. Quelle ist eine Applikationen im lokalen Netz. Ziel ist eine externe Gegenstelle z.B. im Internet oder in einem privaten Netz.

Entsprechend der Werkseinstellung ist zunächst keine ausgehende Firewall-Regel gesetzt, d.h. es dürfen keine IP-Pakete passieren.

Neu Fügt eine weitere Firewall-Regel hinzu, die Sie dann ausfüllen können.

Protokoll Wählen Sie das Protokoll aus, für das diese Regel gelten soll. Zur Auswahl stehen *TCP, UDP, ICMP*. Wenn Sie *Alle* wählen, gilt die Regel für alle drei Protokolle.

Von IP Tragen Sie die IP-Adresse der lokalen Applikation ein, die IP-Pakete zum externen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der lokalen Applikation an. ***0.0.0.0/0*** bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

	Von Port	Tragen Sie den Port ein, von dem die lokale Applikation IP-Pakete senden darf. Geben Sie dazu die Portnummer an. (wird nur ausgewertet bei den Protokollen TCP und UDP)
	Nach IP	Tragen Sie ein, an welche IP-Adresse im externen Netz IP-Pakete gesendet werden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Applikation im Netz an. ***0.0.0.0/0*** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.
	Nach Port	Tragen Sie ein, an welchen Port die lokale Applikation IP-Pakete senden darf. Geben Sie dazu die Portnummer an. (wird nur ausgewertet bei den Protokollen TCP und UDP)
	Aktion	Wählen Sie aus, wie mit abgehenden IP-Paketen zu verfahren ist: Erlauben – Die Datenpakete dürfen passieren, Zurückweisen – Die Datenpakete werden abgewiesen, der Absender erhält eine entsprechende Meldung, Verwerfen – Die Datenpakete werden ohne Rückmeldung an den Absender verworfen.
Firewall-Regeln Ein-/ Ausgehend	*Log*	Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel - das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen - oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung) Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.
Log-Einträge für unbekannte Verbindungsversuche	Damit werden alle Verbindungsversuche protokolliert, die nicht von den festgelegten Regeln erfasst werden.	

Werkseinstellung

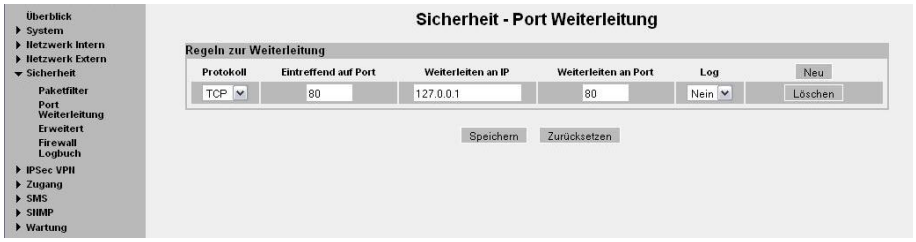
Werkseitig hat das TAINY xMOD folgende Einstellungen:

Firewall eingehend	Firewall-Regeln Eingehend	**- (Alles gesperrt)**
	Protokoll	**Alle**
	Von IP	**0.0.0.0/0**
	Von Port	**ANY**
	Nach IP	**0.0.0.0/0**
	Nach Port	**ANY**
	Aktion	**Erlauben**
	Log	**Nein (Ausgeschaltet)**
	Log-Einträge für unbekannte Verbindungsversuche	**Nein (Ausgeschaltet)**
Firewall ausgehend	Firewall-Regeln Ausgehend	**- (Alles gesperrt)**
	Protokoll	**Alle**
	Von IP	**0.0.0.0/0**
	Von Port	**ANY**

Nach IP	**0.0.0.0/0**
Nach Port	**ANY**
Aktion	**Erlauben**
Log	**Nein (Ausgeschaltet)**
Log-Einträge für unbekannte Verbindungsversuche	**Nein (Ausgeschaltet)**

6.2 Port Weiterleitung

Sicherheit > Port Weiterleitung



Funktion

Ist eine Regel zur Port-Weiterleitung erstellt, dann werden Datenpakete, die aus dem externen Netz auf einem festgelegten IP-Port des TAINY xMOD eintreffen, weitergeleitet. Die eingehenden Datenpakete werden dann weitergeleitet an eine festgelegte IP-Adresse und Port-Nummer im lokalen Netz. Die Port-Weiterleitung kann für TCP oder UDP konfiguriert werden.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse des TAINY xMOD sowie an einen bestimmten Port gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden.
D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT oder Port Forwarding genannt.

Hinweis

Damit ankommende Datenpakete an die festgelegte IP-Adresse im lokalen Netz weitergeleitet werden können, muss für diese IP-Adresse eine entsprechende eingehende Firewall-Regel im Paketfilter eingerichtet werden. Siehe Kapitel 6.1.

Neu	Fügt eine neue Weiterleitungs-Regel hinzu, die Sie dann ausfüllen können.
Löschen	Entfernt angelegte Weiterleitungs-Regeln wieder.
Protokoll	Geben Sie hier das Protokoll (TCP oder UDP) an, auf das sich die Regel beziehen soll.
Eintreffend auf Port	Geben Sie hier die Portnummer (z.B. 80) an, auf dem die Datenpakete aus dem externen Netz eintreffen, die weitergeleitet werden sollen.
Weiterleiten an IP	Geben Sie hier die IP-Adresse im lokalen Netz an, an den die eintreffenden Datenpakete weitergeleitet werden sollen.
Weiterleiten an Port	Geben Sie hier die Portnummer (z.B. 80) zur IP-Adresse im lokalen Netz an, an den die eintreffenden Datenpakete weitergeleitet werden sollen.

Log Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
- oder nicht - *Log* auf *Nein* setzen (Werkseinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Regeln zur Weiterleitung	**-**
Protokoll	**TCP**
Eintreffend auf Port	**80**
Weiterleiten an IP	**127.0.0.1**
Weiterleiten an Port	**80**
Log	**Nein (Ausgeschaltet)**

6.3 Erweiterte Sicherheitsfunktionen

Sicherheit > Erweitert

Funktion

Die erweiterten Sicherheitsfunktionen dienen dazu, das TAINY xMOD und die lokalen Applikationen gegen Angriffe zu schützen. Zum Schutz wird angenommen, dass nur eine bestimmte Anzahl von Verbindungen oder empfangener PING-Pakete im normalen Betrieb zulässig und erwünscht sind, und dass bei einer plötzlichen Häufung ein Angriff stattfindet.

Maximale Zahl …

Die Einträge

- Maximale Zahl gleichzeitiger Verbindungen
- Maximale Zahl neuer eingehender TCP-Verbindungen pro Sekunde
- Maximale Zahl neuer ausgehender TCP-Verbindungen pro Sekunde
- Maximale Zahl neuer eingehender Ping-Pakete pro Sekunde
- Maximale Zahl neuer ausgehender Ping-Pakete pro Sekunde

legen Obergrenzen fest. Die Voreinstellungen (siehe Abbildung) sind so gewählt, dass sie bei normalem praktischem Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte entsprechend ändern.

ICMP von extern zum TAINY

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Paketen beeinflussen, die aus dem externen Netz in Richtung des TAINY xMOD gesendet werden. Sie haben folgende Möglichkeiten:

- *Verwerfen*: Alle ICMP-Pakete zum TAINY xMOD werden verworfen.
- *Ping Erlauben*: Nur Ping-Pakete (ICMP Typ 8) zum TAINY xMOD werden akzeptiert.
- *Erlauben*: Alle Typen von ICMP-Pakete TAINY xMOD werden akzeptiert.

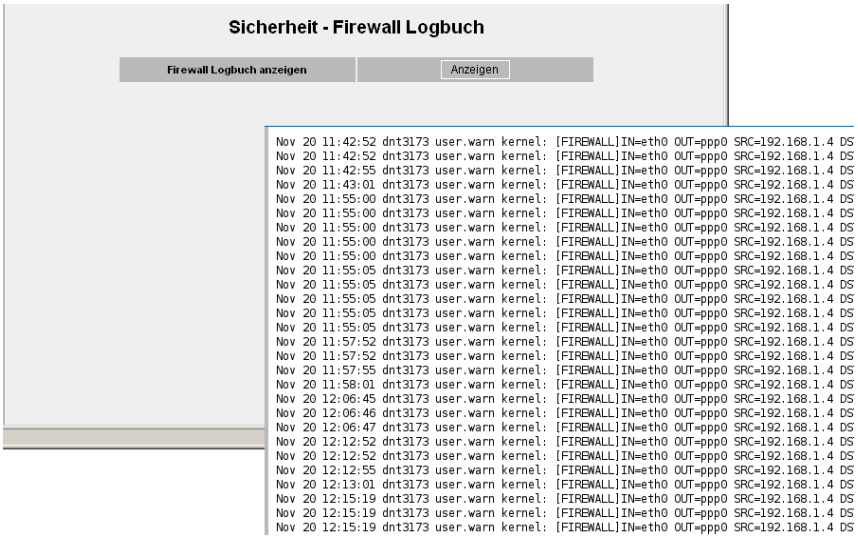
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Maximale Zahl gleichzeitiger Verbindungen	**4096**
Maximale Zahl neuer eingehender TCP-Verbindungen pro Sekunde	**25**
Maximale Zahl neuer ausgehender TCP-Verbindungen pro Sekunde	**75**
Maximale Zahl neuer eingehender Ping-Pakete pro Sekunde	**3**
Maximale Zahl neuer ausgehender Ping-Pakete pro Sekunde	**5**
ICMP von extern zum TAINY	**Verwerfen**

6.4 Firewall-Logbuch

Sicherheit > Firewall Logbuch



Funktion

Im Firewall-Logbuch wird eingetragen, wann einzelne Firewall-Regeln angewendet wurden. Dazu muss zu den verschiedenen Firewall-Funktionen die LOG-Funktion aktiviert werden.

Achtung

Das Firewall-Logbuch geht bei einem Neustart verloren.

7 VPN-Verbindungen

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO

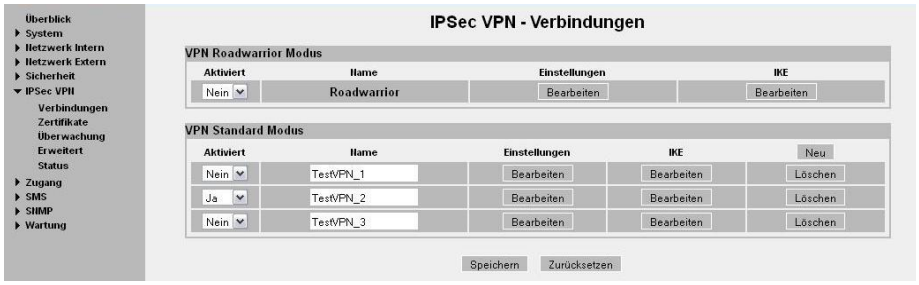
Hinweis zum Funktionsumfang

Der Menüpunkt IPsec-VPN findet sich nur beim TAINY HMOD-V2-IO und TAINY EMOD-V2-IO. Nur das TAINY HMOD-V2-IO und TAINY EMOD-V2-IO unterstützen IPsec-VPN-Verbindungen.

7.1 Einleitung

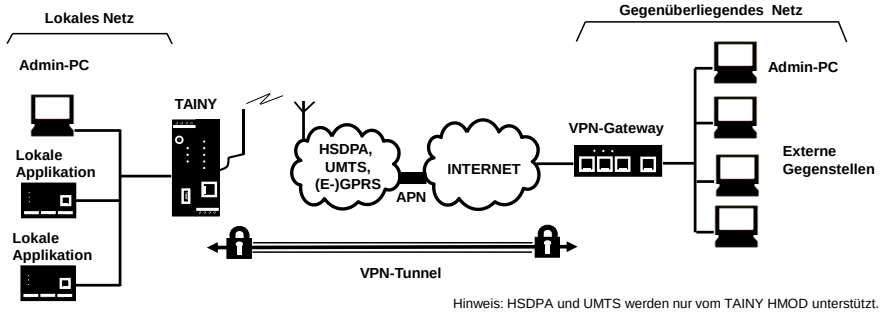
IPsec-VPN > Verbindungen

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



Funktion

Das TAINY xMOD-V2-IO kann das lokale Netz über einen VPN-Tunnel mit einem befreundeten gegenüberliegenden Netz verbinden. Die IP-Datenpakete, die zwischen den beiden Netzen ausgetauscht werden, werden verschlüsselt und sind durch den VPN-Tunnel gegen unerlaubte Manipulationen geschützt. So können auch ungeschützte öffentliche Netze wie das Internet zum Transport der Daten verwendet werden, ohne die Vertraulichkeit oder Integrität der Daten zu gefährden.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Damit das TAINY xMOD-V2-IO einen VPN-Tunnel aufbauen kann, muss das gegenüberliegende Netz über ein VPN-Gateway als Gegenstation des TAINY xMOD-V2-IO verfügen.

Das TAINY xMOD-V2-IO verwendet für den VPN-Tunnel das IPsec-Verfahren im Tunnelmodus. Dabei werden die zu übertragenden IP-Datenpakete vollkommen verschlüsselt und mit einem neuen Header versehen, bevor sie zum VPN-Gateway der Gegenstelle gesendet werden. Dort werden die empfangenen Datapakete entschlüsselt und aus ihnen die ursprünglichen Datapakete wiederhergestellt. Diese werden dann zum Ziel im gegenüberliegenden Netz weitergeleitet.

Unterschieden werden zwei Modi der VPN-Verbindungen:

- Im VPN Roadwarrior-Modus kann das TAINY xMOD-V2-IO VPN-Verbindungen von Gegenstellen mit unbekannter Adresse annehmen. Das können zum Beispiel Gegenstellen im mobilen Einsatz sein, die ihre IP-Adresse dynamisch beziehen. Das TAINY xMOD-V2-IO selbst muss über eine feste IP oder über einen DynDNS-Dienst (siehe Kapitel 5.3 und 5.4) erreichbar sein.
  Die VPN-Verbindung muss durch die Gegenstelle aufgebaut werden.
  Es ist nur eine VPN-Verbindung im Roadwarrior-Modus möglich.
  VPN-Verbindungen im Standard-Modus können dazu parallel betrieben werden.
- Im VPN Standard-Modus muss die Adresse (IP-Adresse oder Hostname) des VPN-Gateways der Gegenstelle bekannt sein, damit die VPN-Verbindung aufgebaut werden kann. Die VPN-Verbindung kann wahlweise aufgebaut werden durch das TAINY xMOD-V2-IO oder durch das VPN-Gateway der Gegenstelle.

Der Aufbau der VPN-Verbindung ist in zwei Phasen aufgeteilt. Zunächst wird in der Phase 1 (ISAKMP = Internet Security Association and Key Management Protocol) die Sicherheitsbeziehung (SA = Security Association) für den Schlüsselaustausch zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle aufgebaut.

Danach wird dann in der Phase 2 (IPsec = Internet Protocol Security) die Sicherheitsbeziehung (SA = Security Association) für die eigentlichen IPsec-Verbindung zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle aufgebaut.

Anforderungen an das VPN-Gateway des gegenüberliegenden Netzes

Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:

- Authentifizierung über X.509-Zertifikate, CA-Zertifikate oder Pre-Shared Key (PSK)
- ESP
- Diffie-Hellman Gruppe 1, 2 oder 5
- 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel Mode
- Quick Mode
- Main Mode / Agressive Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

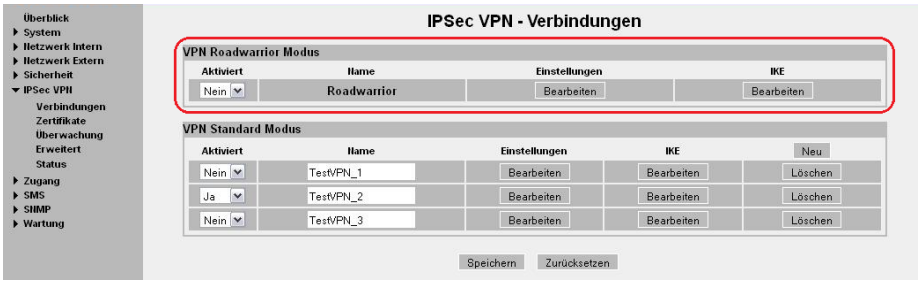
Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das Microsoft Windows 2000 High Encryption Pack oder mindestens das Service Pack 2 installiert sein.

Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough).

7.2 VPN Roadwarrior-Modus

IPsec-VPN > Verbindungen

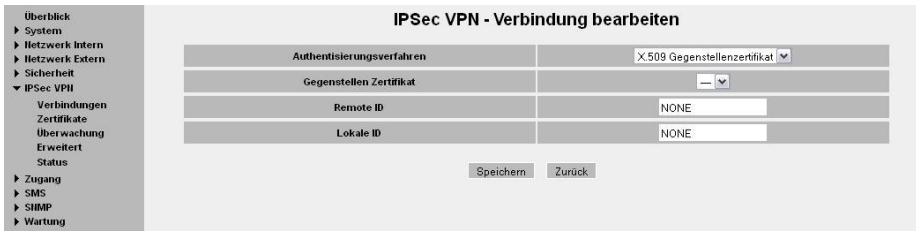
NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



Funktion

Der Roadwarrior-Modus ermöglicht dem TAINY xMOD-V2-IO die Annahme einer VPN-Verbindung, die von einer Gegenstelle mit unbekannter IP-Adresse eingeleitet wird. Die Gegenstelle muss sich korrekt authentifizieren; auf die Identifikation der Gegenstelle anhand der IP-Adresse oder des Hostnamens der Gegenstelle wird bei dieser VPN-Verbindung aber verzichtet.

Roadwarrior-Modus Einstellungen bearbeiten



Funktion

Richten Sie das TAINY xMOD-V2-IO entsprechend den Absprachen mit dem Systemadministrator der Gegenstelle ein.

Authentifizierungs-verfahren

Wählen Sie das Authentifizierungsverfahren entsprechend Ihren Vereinbarungen mit dem Administrator der Gegenstelle.

Das TAINY xMOD-V2-IO unterstützt drei Verfahren:

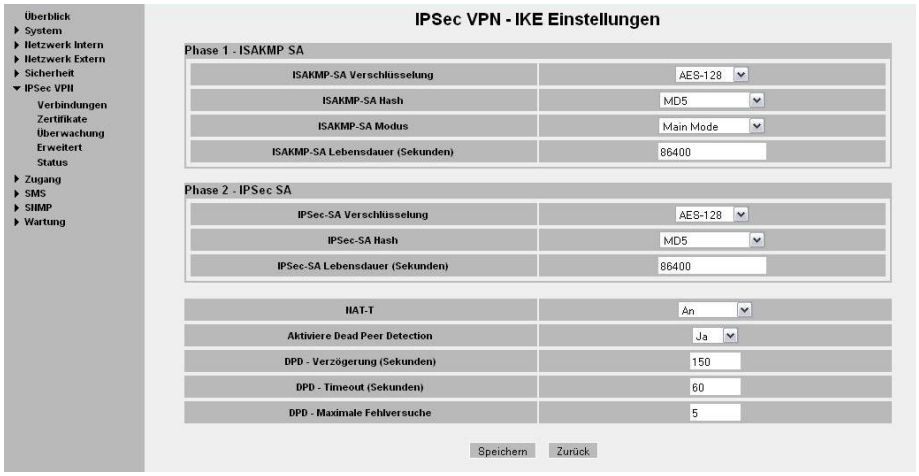
- X.509-Zertifikat
- CA-Zertifikat
- Pre-Shared Key

X.509-Zertifikat, CA-Zertifikat

Bei den Authentifizierungsverfahren X.509-Zertifikat und CA-Zertifikat werden zur Authentifikation Schlüssel verwendet, die zuvor durch eine zertifizierende Stelle (CA = Certification Authority) signiert wurden. Diese Verfahren gelten als besonders sicher. Eine CA kann ein Dienstleister sein, aber z.B. auch der System-Administrator Ihres Projektes, sofern dieser über die notwendigen Software-Werkzeuge verfügt. Die CA erstellt für beide Gegenstellen einer VPN-Verbindung je eine Zertifikatsdatei (PKCS12) mit der Dateiendung *p12. Diese Zertifikatsdatei enthält den öffentlichen und privaten Schlüssel der eigenen Station, das signierte Zertifikat der CA und den öffentlichen Schlüssel der CA. Für das Authentifizierungsverfahren X.509 gibt es zusätzlich für jede der beiden Gegenstellen noch eine Schlüsseldatei (*.pem oder *.crt) mit dem öffentlichen Schlüssel der eigenen Station.

	X.509-Zertifikat: Der Austausch der öffentlichen Schlüssel (Datei mit Endung *.pem oder *.crt) zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle erfolgt manuell, zum Beispiel per CD-ROM oder per E-Mail. Zum Laden des Zertifikates gehen Sie vor, wie im Kapitel 7.4 beschrieben.
	CA-Zertifikat: Der Austausch der öffentlichen Schlüssel zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle erfolgt über die Datenverbindung beim Aufbau der VPN-Verbindung. Ein manueller Austausch von Schlüsseldateien entfällt.
	Pre-Shared Secret Key (PSK) Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei erfolgt die Authentifikation mit einer zuvor verabredeten Zeichenfolge. Um eine hohe Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen. Folgende Zeichen sind erlaubt: ! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | } # Die Eingabe erfolgt verdeckt.
Gegenstellen Zertifikat	Haben Sie als Authentifizierungsverfahren X.509-Zertifikat gewählt, wird hier die Liste der Zertifikate der Gegenstellen angezeigt, die Sie bereits in das TAINY xMOD-V2-IO geladen haben. Wählen Sie das Zertifikat für die VPN-Verbindung aus.
Remote-ID Lokale ID	Die Lokale ID und die Remote-ID werden vom IPsec genutzt, um beim Aufbau der VPN-Verbindung die Gegenstellen eindeutig zu identifizieren. Die eigene Lokale ID bildet die Remote-ID der Gegenstelle und umgekehrt. Bei Authentifizierung mit X.509-Zertifikat oder CA-Zertifikat: - Beläßt man die Werkseinstellung *NONE*, so werden als Lokale ID und Remote-ID automatisch die Distinguished Names aus dem eigenen Zertifikat und aus dem von der Gegenstelle übermittelten Zertifikat übernommen. - Ändert man manuell den Eintrag für die Lokale ID oder die Remote-ID, so müssen die korrespondierenden Einträge der Gegenstelle angepasst werden. Der manuelle Eintrag für Lokale oder Remote-ID muss im ASN.1-Format erfolgen, z.B. "C=XY/O=XY Org/CN=xy.org.org" Bei Authentifizierung mit Pre-Shared Secret Key (PSK): - Im Roadwarrior-Modus, muss manuell die Remote-ID eingetragen werden. Die Remote-ID muss das Format eines Hostnames (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben und mit der Lokalen ID der Gegenstelle übereinstimmen. Die Lokale ID kann auf *NONE* belassen werden. In diesem Fall wird die IP-Adresse als lokale IP-Adresse verwendet. Trägt man eine Lokale ID ein, muss diese das Format eines Hostnames (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben und mit der Remote-ID der Gegenstelle übereinstimmen.

Roadwarrior-Modus IKE bearbeiten



Funktion

Definieren Sie hier die Eigenschaften der VPN-Verbindung entsprechend Ihren Anforderungen und den Absprachen mit dem Administrator der Gegenstelle.

ISAKMP-SA Verschlüsselung

IPSec-SA Verschlüsselung

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll für die ISAKMP-SA und die IPSec-SA. Das TAINY xMOD-V2-IO unterstützt die folgenden Verfahren:

- 3DES-192
- AES-128
- AES-192
- AES-256

AES-128 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Das Verfahren kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

Hinweis:
Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das Verfahren AES-256 Verfahren gilt daher als am sichersten. Allerdings ist der Verschlüsselungsvorgang umso zeitaufwendiger und benötigt mehr Rechenleistung, je länger der Schlüssel ist.

ISAKMP-SA Hash

IPSec-SA Hash

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Berechnung von Prüfsummen/Hash während der ISAKMP-Phase und der IPSec-Phase verwendet werden soll. Zur Auswahl stehen:

- MD5 oder SHA-1 (Automatische Erkennung)
- MD5
- SHA-1

Das Verfahren kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

ISAKMP-SA Modus

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Aushandlung der ISAKMP-SA verwendet werden soll. Zur Auswahl stehen:

- Main mode
- Agressive mode

Hinweis:

Bei Verwendung des Authentifizierungsverfahren Pre-Shared Key muss im Roadwarrior-Modus der Agressive mode eingestellt werden.

ISAKMP-SA-Lebensdauer

IPSec-SA Lebensdauer

Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um den Aufwand eines Angriffs auf eine IPsec-Verbindung zu erhöhen.

Legen Sie die Lebensdauer der für die ISAKMP-SA und IPSec-SA vereinbarten Schlüssel fest (in Sekunden).

Die Lebensdauer kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

NAT-T

Eventuell befindet sich zwischen dem TAINY xMOD-V2-IO und den VPN-Gateway des gegenüberliegenden Netzes ein NAT-Router. Nicht alle NAT-Router lassen IPsec-Datenpakete passieren. Daher ist es eventuell erforderlich die IPsec-Datenpakete in UPD-Pakete einzukapseln, so dass sie den NAT-Router passieren können.

An: Wird vom TAINY xMOD-V2-IO ein NAT-Router erkannt, der die IPsec-Datenpakete nicht passieren lässt, startet automatisch die UDP-Kapselung.

Erzwingen: Bei Aushandlung der Verbindungsparameter der VPN-Verbindung wird darauf bestanden, dass während der Verbindung die Datenpakete gekapselt übertragen werden.

Aus: Die NAT-T-Funktion ist ausgeschaltet

Aktiviere Dead Peer Detection

Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA-Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden. Um zu prüfen, ob die IPsec-Verbindung noch gültig ist sendet die Dead Peer Detection selber DPD-Anfragen zur Gegenstelle. Gibt es keine Antwort, wird die IPsec-Verbindung nach einer Anzahl von erlaubten Fehlversuchen als unterbrochen angesehen.

Warnung

Durch das Versenden der DPD-Anfragen sowie durch die Nutzung von NAT-T steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSDPA, UMTS, EGPRS, GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen.

Ja Die Dead Peer Detection ist eingeschaltet. Das TAINY xMOD-V2-IO erkennt unabhängig von der Übertragung von Nutzdaten einen Verlust der Verbindung und wartet in diesem Fall auf den Neuaufbau der Verbindung durch die Gegenstellen.

Nein Die Dead Peer Detection ist ausgeschaltet

DPD - Verzögerung (Sekunden)

Zeitspanne in Sekunden, nach welcher DPD-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.

DPD - Timeout (Sekunden)	Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die DPD-Anfragen keine Antwort erfolgte.
DPD – Maximale Fehlversuche	Anzahl der zulässigen Fehlversuche bevor die IPsec-Verbindung als unterbrochen angesehen wird.

Werkseinstellung

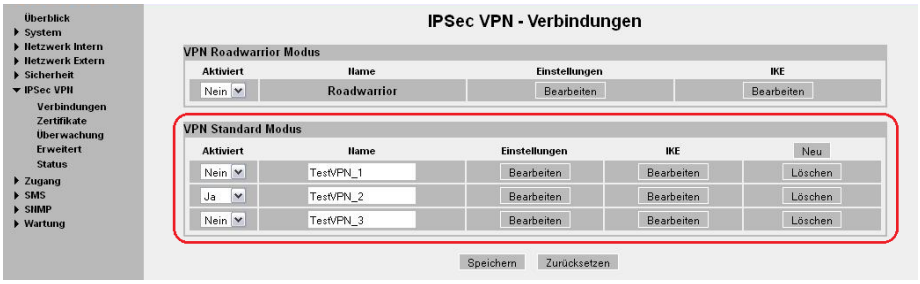
Werkseitig hat das TAINY xMOD-V2-IO folgende Einstellungen:

Name	**Roadwarrior**
Aktiviert	**Nein (Ausgeschaltet)**
Authentifizierungsverfahren	**CA-Zertifikat**
Remote-ID	**NONE**
Lokale ID	**NONE**
Gegenstellen Zertifikat	**-**
ISAKMP-SA Verschlüsselung	**AES-128**
IPSec-SA Verschlüsselung	**AES-128**
ISAKMP-SA Hash	**MD5**
IPSec-SA Hash	**MD5**
ISAKMP-SA Modus	**Main**
ISAKMP-SA-Lebensdauer (Sekunden)	**86400**
IPSec-SA-Lebensdauer (Sekunden)	**86400**
NAT-T	**An**
Aktiviere Dead Peer Detection	**Ja**
DPD - Verzögerung (Sekunden)	**150**
DPD – Timeout (Sekunden)	**60**
DPD – Maximale Fehlversuche	**5**

7.3 VPN IPsec Standard-Modus

IPsec-VPN > Verbindungen

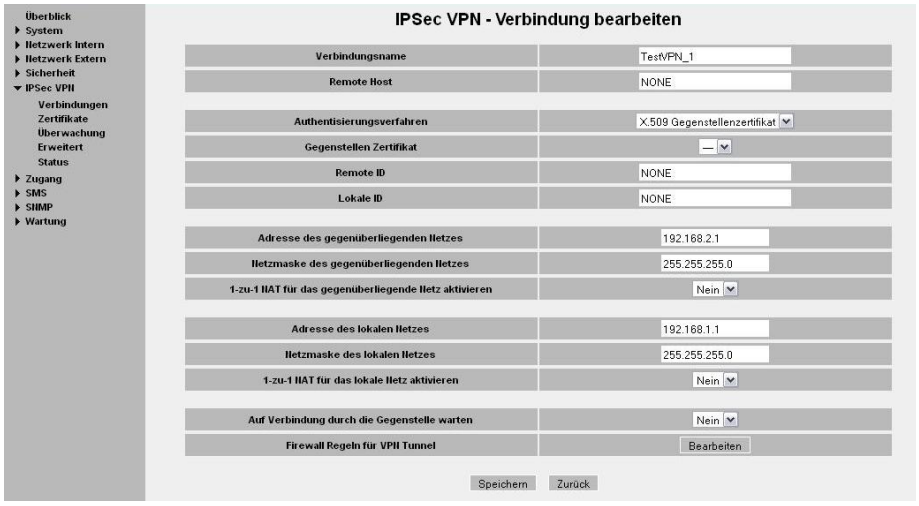
NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



Funktion	Angezeigt werden die bereits angelegten VPN-Verbindungen. Sie können jede einzelne Verbindung aktivieren (Aktiviert = *Ja*) oder deaktivieren (Aktiviert = *Nein*). Mit *Neu* können Sie weitere VPN-Verbindungen hinzufügen, mit *Einstellungen Bearbeiten* und *Erweitert Bearbeiten* können Sie diese einrichten und mit *Löschen* können Sie eine Verbindung entfernen.

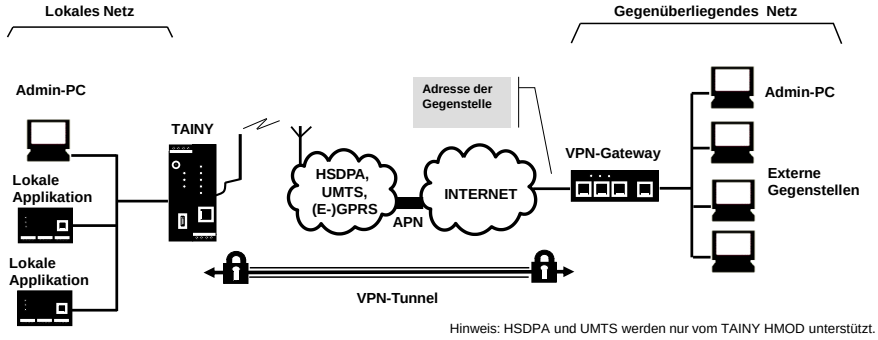
VPN Standard-Modus

Einstellungen bearbeiten



Verbindungsname — Geben Sie der neuen Verbindung hier einen Verbindungsnamen.

Remote Host — Geben Sie hier die Adresse der Gegenstelle an, entweder als Hostname (z.B. myadress.com) oder als IP-Adresse.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

X.509-Zertifikat, CA-Zertifikat

Bei den Authentifizierungsverfahren X.509-Zertifikat und CA-Zertifikat werden zur Authentifikation Schlüssel verwendet, die zuvor durch eine zertifizierende Stelle (CA = Certification Authority) signiert wurden. Diese Verfahren gelten als besonders sicher. Eine CA kann ein Dienstleister sein, aber z.B. auch der System-Administrator Ihres Projektes, sofern dieser über die notwendigen Software-Werkzeuge verfügt. Die CA erstellt für beide Gegenstellen einer VPN-Verbindung je eine Zertifikatsdatei (PKCS12) mit der Dateiendung *p12. Diese Zertifikatsdatei enthält den öffentlichen und privaten Schlüssel der eigenen Station, das signierte Zertifikat der CA und den öffentlichen Schlüssel der CA. Für das Authentifizierungsverfahren X.509 gibt es zusätzlich für jede der beiden Gegenstellen noch eine Schlüsseldatei (*.pem oder *.crt) mit dem öffentlichen Schlüssel der eigenen Station.

X.509-Zertifikat — Der Austausch der öffentlichen Schlüssel (Datei mit Endung *.pem oder *.crt) zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle erfolgt manuell, zum Beispiel per CD-ROM oder per E-Mail. Zum Laden des Zertifikates gehen Sie vor, wie im Kapitel 7.4 beschrieben.

	CA-Zertifikat	Der Austausch der öffentlichen Schlüssel zwischen dem TAINY xMOD-V2-IO und dem VPN-Gateway der Gegenstelle erfolgt über die Datenverbindung beim Aufbau der VPN-Verbindung. Ein manueller Austausch von Schlüsseldateien entfällt.

Pre-Shared Secret Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei erfolgt die Authentifikation mit einer zuvor verabredeten Zeichenfolge. Um eine hohe Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

Folgende Zeichen sind erlaubt:

! $ % & ' ( ) * + , . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ ` a b c d e f g h I j k l m n o p q r s t u v w x y z { | } #

Die Eingabe erfolgt verdeckt.

Remote-ID

Lokale ID

Die Lokale ID und die Remote-ID werden vom IPsec genutzt, um beim Aufbau der VPN-Verbindung die Gegenstellen eindeutig zu identifizieren.

Bei Authentifizierung mit X.509-Zertifikat oder CA-Zertifikat:

- Beläßt man die Werkseinstellung *NONE*, so werden als Lokale ID und Remote-ID automatisch die Distinguished Names aus dem eigenen Zertifikat und aus dem von der Gegenstelle übermittelten Zertifikat übernommen und verwendet.
- Ändert man manuell den Eintrag für die Lokale ID oder die Remote-ID, so müssen die korrespondierenden Einträge der Gegenstelle angepasst werden. Die eigene Lokale ID muss mit der Remote-ID der Gegenstelle übereinstimmen und umgekehrt. Die Einträge für Lokale oder Remote-ID müssen im ASN.1-Format erfolgen, z.B. "C=XY/O=XY Org/CN=xy.org.org"

Bei Authentifizierung mit Pre-Shared Secret Key (PSK):

- Beläßt man die Werkseinstellung *NONE*, so werden automatisch als Lokale ID die eigene IP-Adresse und als Remote-ID die IP-Adresse der Gegenstelle übernommen.
- Ändert man manuell den Eintrag für die Lokale ID oder für die Remote-ID, so müssen die Einträge das Format eines Hostnames (z.B. RemoteStation.de) oder das Format einer E-Mail-Adresse (remote@station.de) haben. Die eigene Lokale ID muss mit der Remote-ID der Gegenstelle übereinstimmen und umgekehrt.

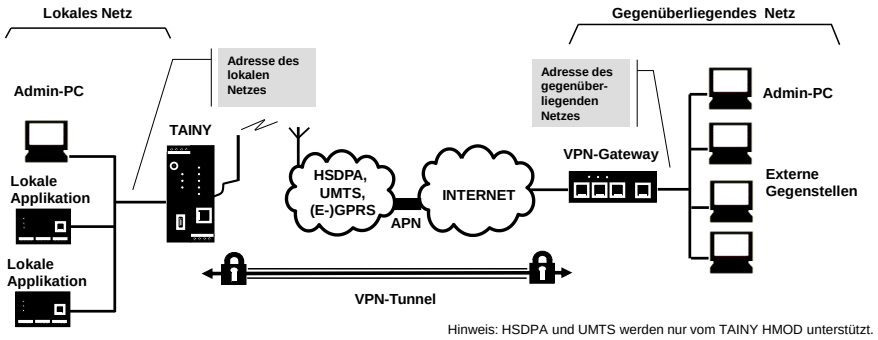
Hinweis:

Wenn bei Pre-Shared Secret Key (PSK) nicht die IP-Adresse als Remote-ID verwendet wird, muss als ISAKMP-SA-Modus der Agressive mode eingestellt werden.

Auf Verbindung durch die Gegenstelle warten	*Ja*	Das TAINY xMOD-V2-IO wartet darauf, dass das VPN-Gateway des gegenüberliegenden Netzes den Aufbau der VPN-Verbindung einleitet.
	Nein	Das TAINY xMOD-V2-IO leitet den Verbindungsaufbau ein.

Adresse des gegenüberliegenden Netzes

Tragen Sie hier die IP-Adresse (z.B. 123.123.123.123) des gegenüberliegenden Netzes ein. Das gegenüberliegende Netz kann auch nur ein einzelner Rechner sein.



Hinweis: HSDPA und UMTS werden nur vom TAINY HMOD unterstützt.

Netzmaske des gegenüberliegenden Netzes

Tragen Sie hier die Netzwerkmaske (z.B. 255.255.255.0) des gegenüberliegenden Netzes ein. Das gegenüberliegende Netz kann auch nur ein einzelner Rechner sein.

1-zu-1-NAT für das gegenüberliegende Netz aktivieren

Das TAINY xMOD-V2-IO verfügt über eine 1-zu-1-NAT-Funktion zum gegenüberliegende Netz.

Der Adressbereich des gegenüberliegenden Netzes auf der VPN-Verbindung wird im TAINY xMOD-V2-IO festgelegt über die

- Adresse des gegenüberliegenden Netzes und die
- Netzmaske des gegenüberliegenden Netzes

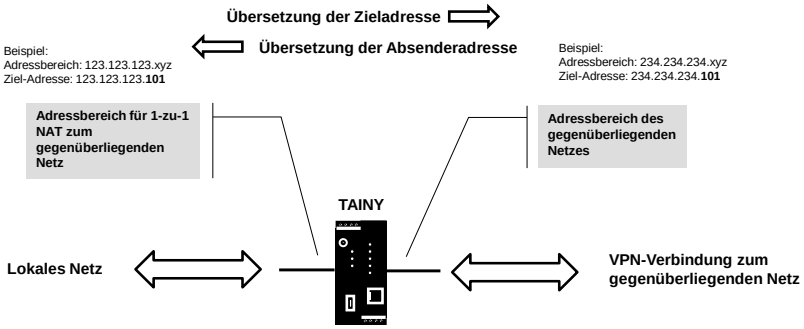
Ist 1-zu-1-NAT abgeschaltet, müssen lokale Applikationen diesen Adressbereich zur Adressierung von Gegenstellen im gegenüberliegenden Netz verwenden.

Ist 1-zu-1-NAT aktiviert, kann ein lokal verwendeter Adressbereich definiert werden, über den lokale Applikationen die Gegenstellen im gegenüberliegenden Netz adressieren können.

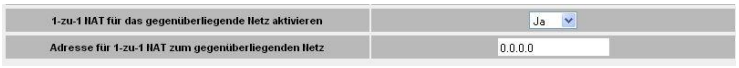
Die 1-zu-1-NAT-Funktion im TAINY xMOD-V2-IO bildet dann den lokal definierten Adressbereich des gegenüberliegenden Netzes auf den Adressbereich des gegenüberliegenden Netzes auf der VPN-Verbindung ab.

Der lokal verwendete Adressbereich des gegenüberliegenden Netzes wird festgelegt über die

- Adresse für 1-zu-1-NAT zum gegenüberliegenden Netz und die
- Netzmaske des gegenüberliegenden Netzes



Ja Das TAINY xMOD-V2-IO verwendet 1-zu-1-NAT zum gegenüberliegenden Netz.



Geben Sie als Adresse für 1-zu-1-NAT zum gegenüberliegenden Netz die lokal verwendete Zieladresse ein.

Nein Das TAINY xMOD-V2-IO verwendet kein 1-zu-1-NAT zum gegenüberliegenden Netz.

Adresse des lokalen Netzes — Tragen Sie hier die IP-Adresse (z.B. 123.123.123.123) des lokalen Netzes ein. Das lokale Netz kann auch nur ein einzelner Rechner sein.

Netzmaske des lokalen Netzes — Tragen Sie hier die Netzwerkmaske (z.B. 255.255.255.0) des lokalen Netzes ein. Das lokale Netz kann auch nur ein einzelner Rechner sein.

1-zu-1-NAT für das lokale Netz aktivieren — Der Adressbereich des lokalen Netzes auf der VPN-Verbindung wird im TAINY xMOD-V2-IO festgelegt über die

Adresse des lokalen Netzes und die

Netzmaske des lokalen Netzes

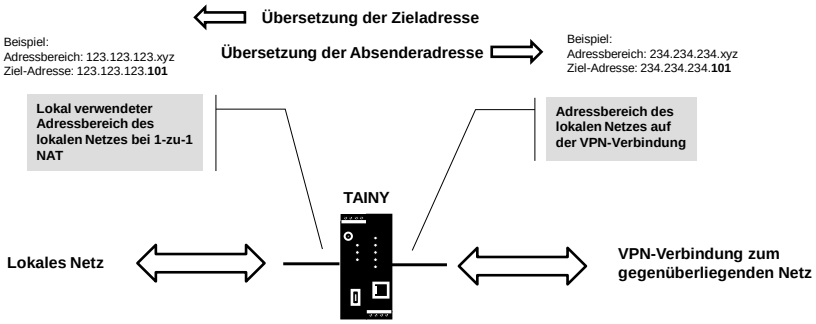
Ist 1-zu-1-NAT abgeschaltet, müssen die Adressen lokaler Applikationen in diesem Adressbereich liegen, um über die VPN-Verbindung von Gegenstellen im gegenüberliegenden Netz adressiert werden zu können.

Ist 1-zu-1-NAT aktiviert, kann ein lokal verwendeter Adressbereich für das lokale Netz definiert werden, der sich von dem Adressbereich, der auf der VPN-Verbindung genutzt wird unterscheidet.

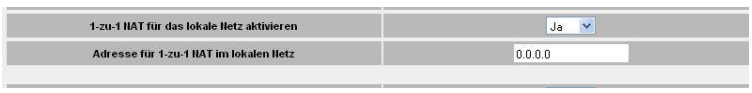
Die 1-zu-1-NAT-Funktion im TAINY xMOD-V2-IO bildet dann den lokalen Adressbereich des lokalen Netzes auf den Adressbereich des lokalen Netzen auf der VPN-Verbindung ab.

Der lokal verwendete Adressbereich des lokalen Netzes wird festgelegt über die

- Adresse für 1-zu-1-NAT im lokalen Netz und die
- Netzmaske des lokalen Netzes



Ja Das TAINY xMOD-V2-IO verwendet 1-zu-1-NAT zum lokalen Netz.



Geben Sie als Adresse für 1-zu-1-NAT im lokalen Netz die lokal verwendete Zieladresse ein.

Nein Das TAINY xMOD-V2-IO verwendet kein 1-zu-1-NAT zum lokalen Netz.

Firewall-Regeln für VPN-Tunnel

Siehe Kapitel 7.5

VPN Standard-Modus

IKE bearbeiten

Funktion

Definieren Sie hier die Eigenschaften der VPN-Verbindung entsprechend Ihren Anforderungen und den Absprachen mit dem Administrator der Gegenstelle.

ISAKMP-SA Verschlüsselung

IPSec-SA Verschlüsselung

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll für die ISAKMP-SA und die IPSec-SA. Das TAINY xMOD-V2-IO unterstützt die folgenden Verfahren:

- 3DES-192
- AES-128
- AES-192
- AES-256

AES-128 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Das Verfahren kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

Hinweis:
Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das Verfahren AES-256 Verfahren gilt daher als am sichersten. Allerdings ist der Verschlüsselungsvorgang umso zeitaufwendiger und benötigt mehr Rechenleistung, je länger der Schlüssel ist.

ISAKMP-SA Hash

IPSec-SA Hash

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Berechnung von Prüfsummen/Hash während der ISAKMP-Phase und der IPSec-Phase verwendet werden soll. Zur Auswahl stehen:

- MD5 oder SHA-1 (Automatische Erkennung)
- MD5
- SHA-1

Das Verfahren kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

ISAKMP-SA Modus

Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verfahren zur Aushandlung der ISAKMP-SA verwendet werden soll. Zur Auswahl stehen:

- Main mode
- Agressive mode

DH/PFS-Gruppe

Vereinbaren Sie mit dem Administrator der Gegenstelle die DH-Gruppe für den Schlüsselaustausch.

ISAKMP-SA-Lebensdauer

IPSec-SA Lebensdauer

Die Schlüssel einer IPsec-Verbindung werden in bestimmten Abständen erneuert, um den Aufwand eines Angriffs auf eine IPsec-Verbindung zu erhöhen.

Legen Sie die Lebensdauer der für die ISAKMP-SA und IPSec-SA vereinbarten Schlüssel fest (in Sekunden).

Die Lebensdauer kann für ISAKMP-SA und IPSec-SA unterschiedlich festgelegt werden.

NAT-T

Eventuell befindet sich zwischen dem TAINY xMOD-V2-IO und den VPN-Gateway des gegenüberliegenden Netzes ein NAT-Router. Nicht alle NAT-Router lassen IPsec-Datenpakete passieren. Daher ist es eventuell erforderlich die IPsec-Datenpakete in UPD-Pakete einzukapseln, um den NAT-Router passieren zu können.

An: Wird vom TAINY xMOD-V2-IO ein NAT-Router erkannt, der die IPsec-Datenpakete nicht passieren lässt, startet automatisch die UDP-Kapselung.

Erzwingen: Bei Aushandlung der Verbindungsparameter der VPN-Verbindung wird darauf bestanden, dass während der Verbindung die Datenpakete gekapselt übertragen werden.

Aus: Die NAT-T-Funktion ist ausgeschaltet

Aktiviere Dead Peer Detection

Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec-Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss. Ohne DPD muss je nach Konfiguration bis zum Ablauf der SA-Lebensdauer gewartet oder die Verbindung manuell neu initiiert werden. Um zu prüfen, ob die IPsec-Verbindung noch gültig ist sendet die Dead Peer Detection selber DPD-Anfragen zur Gegenstelle. Gibt es keine Antwort, wird die IPsec-Verbindung nach einer Anzahl von erlaubten Fehlversuchen als unterbrochen angesehen.

Warnung

Durch das Versenden der DPD-Anfragen sowie durch die Nutzung von NAT-T steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSDPA, UMTS, EGPRS, GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen.

Ja Die Dead Peer Detection ist eingeschaltet. Es wird versucht, die IPsec-Verbindung neu aufzubauen, wenn diese für tot erklärt wurde, unabhängig von der Übertragung von Nutzdaten.

Nein Die Dead Peer Detection ausgeschaltet

DPD - Verzögerung (Sekunden)

Zeitspanne in Sekunden, nach welcher DPD-Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.

DPD - Timeout (Sekunden)

Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die DPD-Anfragen keine Antwort erfolgte.

DPD – Maximale Fehlversuche	Anzahl der zulässigen Fehlversuche bevor die IPsec-Verbindung als unterbrochen angesehen wird.

Werkseinstellung

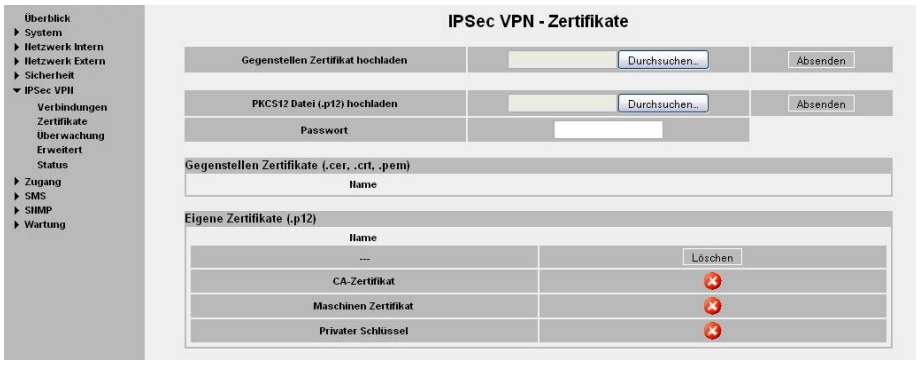
Werkseitig verwendet das TAINY xMOD-V2-IO folgende Einstellungen für eine neu angelegte Verbindung:

Name	**NewConnection**
Aktiviert	**Nein (Ausgeschaltet)**
Authentifizierungsverfahren	**CA-Zertifikat**
Remote-ID	**NONE**
Lokale ID	**NONE**
Gegenstellen Zertifikat	**-**
Auf Verbindung durch die Gegenstelle warten	**Nein**
Adresse des gegenüberliegenden Netzes	**192.168.2.1**
Netzmaske des gegenüberliegenden Netzes	**255.255.255.0**
Adresse des lokalen Netzes	**192.168.1.1**
Netzmaske des lokalen Netzes	**255.255.255.0**
ISAKMP-SA Verschlüsselung	**AES-128**
IPSec-SA Verschlüsselung	**AES-128**
ISAKMP-SA Hash	**MD5**
IPSec-SA Hash	**MD5**
DH/PFS-Gruppe	**DH-2 1024**
ISAKMP-SA Modus	**Main**
ISAKMP-SA-Lebensdauer (Sekunden)	**86400**
IPSec-SA-Lebensdauer (Sekunden)	**86400**
NAT-T	**An**
Aktiviere Dead Peer Detection	**Ja**
DPD - Verzögerung (Sekunden)	**150**
DPD – Timeout (Sekunden)	**60**
DPD – Maximale Fehlversuche	**5**

7.4 VPN Zertifikate laden

IPsec-VPN - Zertifikate

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



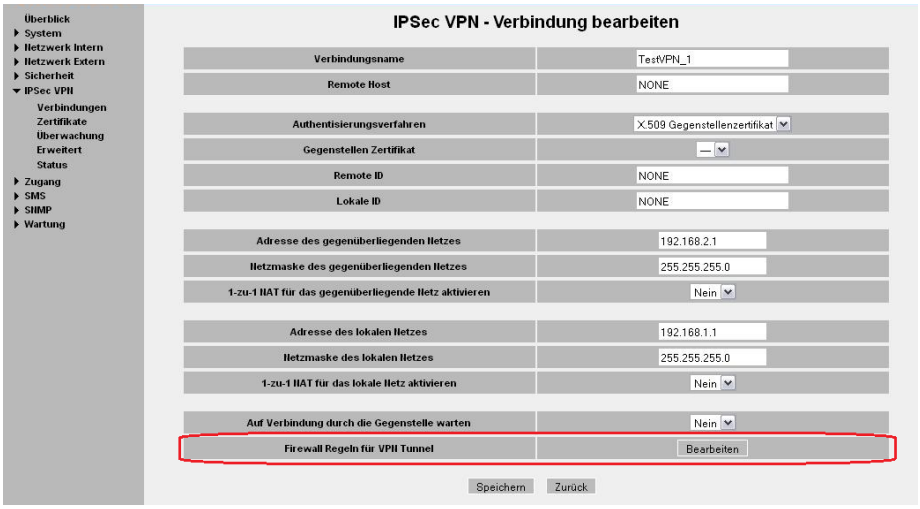
Funktion	Laden und verwalten von Zertifikaten und Schlüsseln.
Gegenstellen Zertifikat hochladen	Laden Sie hier Schlüsseldateien (*.pem, *.crt) mit Gegenstellen-Zertifikaten und öffentlichen Schlüsseln von Gegenstellen in das TAINY xMOD-V2-IO. Die Dateien müssen dazu auf dem Admin-PC gespeichert sein. Ein Gegenstellen-Zertifikat wird nur beim Authentifizierungsverfahren mit X.509-Zertifikat benötigt.
PKCS12 Datei (.p12) hochladen	Laden Sie hier die Zertifikats-Datei (PKCS12-Datei) mit der Dateiendung .p12 in das TAINY xMOD-V2-IO. Die Zertifikats-Datei muss dazu auf dem Admin-PC gespeichert sein.
	Achtung Befindet sich bereits eine Zertifikats-Datei im Gerät, muss diese vor dem Laden einer neuen Datei gelöscht werden.
Passwort	Die Zertifikats-Datei (PKCS12-Datei) ist mit einem Passwort geschützt. Geben Sie hier das Passwort ein, das Sie mit der Zertifikats-Datei erhalten haben.
Gegenstellen Zertifikate (.crt)	An dieser Stelle werden alle geladenen Gegenstellen-Zertifikate in einer Liste angezeigt. Mit *Löschen* können Sie Gegenstellen-Zertifikate, die nicht mehr benötigt werden, wieder entfernen.
Eigene Zertifikate (.p12)	An dieser Stelle wird der Name und Zustand der geladenen Zertifikats-Datei (PKCS12-Datei) angezeigt. Der jeweilige Bestandteil der Zertifikats-Datei vorhanden ist Der jeweilige Bestandteil fehlt oder dass das eingegebene Passwort falsch ist

7.5 Firewall-Regeln für VPN-Tunnel

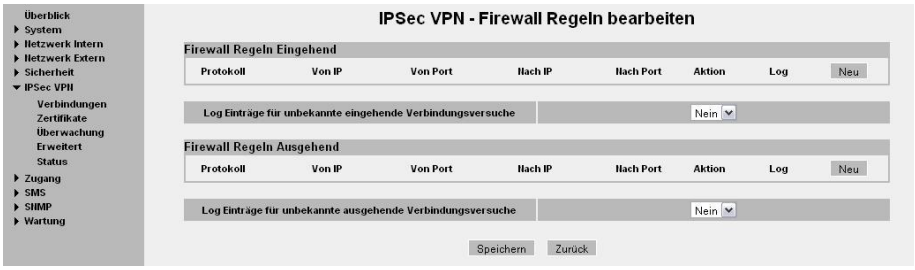
Firewall-Regeln für VPN-Tunnel

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO

Die Oberfläche zum Einrichten der Firewall-Regeln für VPN-Tunnel finden Sie unter IPsec-VPN > Verbindungen:



IPsec-VPN –Firewall-Regeln bearbeiten



Funktion

Die IPsec-VPN-Verbindung wird grundsätzlich als sicher angesehen. So ist der Datenverkehr über diese Verbindung standardmäßig nicht beschränkt. Es ist aber möglich Firewall-Regeln für die VPN-Verbindung zu erstellen

Gehen Sie bei der Einrichtung der Firewall-Regeln für die VPN-Verbindung vor, wie bei der Einrichtung der Paketfilter-Funktion der allgemeinen Firewall (siehe Kapitel 6.1). Die hier festgelegten Regeln, gelten aber nur für die jeweilige VPN-Verbindung.

Werkseinstellung

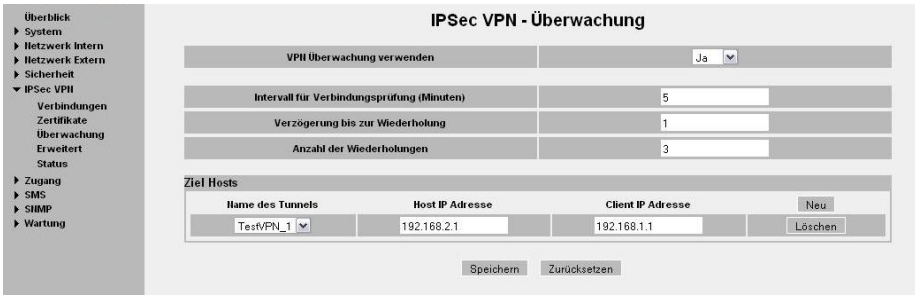
Werkseitig verwendet das TAINY xMOD-V2-IO folgende Einstellungen für eine neu angelegte Verbindung:

Firewall-Regeln für VPN-Tunnel **Keine Beschränkungen**

7.6 Überwachung der VPN-Verbindungen

IPsec-VPN – Überwachung

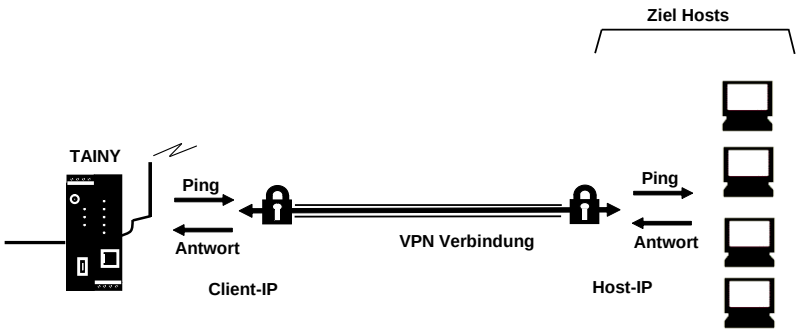
NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



Funktion

Mit der Überwachung der VPN-Verbindungen überprüft das TAINY xMOD-V2-IO aufgebaute VPN-Verbindungen. Dazu sendet das TAINY xMOD-V2-IO über die VPN-Verbindung in regelmäßigen Zeitabständen Ping-Pakete (ICMP) an ein oder mehrere Gegenstellen (Ziel Hosts). Dies geschieht unabhängig von den Nutzdaten. Für jede VPN-Verbindung kann eine eigene Überwachung eingerichtet werden.

Erhält das TAINY xMOD-V2-IO auf einen Ping mindestens von einer der adressierten Gegenstellen eine Antwort, ist die VPN-Verbindung noch funktionsbereit.



Antwortet keine der Gegenstellen auf den Ping, wird nach einer einstellbaren Verzögerung der Ping wiederholt. Enden alle Wiederholungen erfolglos, wird die VPN-Verbindung neu aufgebaut. Schlägt auch das fehl wird dies so oft wiederholt, wie im Menü „IPsec-VPN > Erweitert“ als Parameter *Versuche des Verbindungsaufbaus bis Neustart des Clients* (siehe Kapitel 7.7) konfiguriert ist. Ist die VPN-Verbindung nach allen Wiederholungen noch immer nicht wieder etabliert, wird der VPN-Client neu gestartet. Dies verursacht einen Neuaufbau aller bestehenden VPN-Verbindungen.

Warnung

Durch das Versenden der Ping-Pakete (ICMP) steigt die Anzahl der über die Datenfunkdienst-Verbindung (HSDPA, UMTS, EGPRS oder GPRS) gesendeten und empfangenen Daten. Abhängig von den gewählten Einstellungen kann das zusätzliche Datenaufkommen 4,5 MByte im Monat und mehr betragen. Dies kann zu erhöhten Kosten führen.

Hinweis

Die Überwachung der VPN-Verbindungen mittels Ping überschneidet sich zum Teil mit den Überwachungsfunktionen der Dead Peer Detection. Bei aktivierter Ping-Überwachung kann die DPD – Verzögerung erhöht werden.

VPN-Überwachung verwenden	*Ja*	VPN-Überwachung eingeschaltet
	Nein	VPN-Überwachung ausgeschaltet
Intervall für Verbindungsprüfung	An dieser Stelle wird festgelegt, in welchen Zeitintervallen die Ping-Pakete über die überwachten VPN-Verbindungen (VPN-Tunnel) gesendet werden. Die Angabe erfolgt in Minuten.	
Verzögerung bis zur Wiederholung	An dieser Stelle wird die Wartezeit festgelegt, bis nach einer erfolglosen Ping-Prüfung (keine Antwort auf den Ping), der Ping wiederholt wird. Die Angabe erfolgt in Minuten.	
Anzahl der Wiederholungen	An dieser Stelle wird die Anzahl der erfolglosen Ping-Wiederholungen festgelegt, nach denen die überwachte VPN-Verbindung neu gestartet wird.	
Ziel Hosts	*Name des Tunnels*	Legen Sie hier fest, welche VPN-Verbindungen (VPN-Tunnel) überwacht werden sollen. Richten Sie mit *Neu* für eine der bereits angelegten VPN-Verbindungen eine Überwachung ein oder beenden Sie mit *Löschen* die Überwachung einer VPN-Verbindung.
	Host IP-Adresse	Wählen Sie hierüber deren IP-Adresse die Gegenstelle (Ziel Hosts) aus.
	Client IP-Adresse	Geben Sie hier als Absender IP eine beliebige ungenutzte IP-Adresse aus dem lokalen Netzbereich der jeweiligen VPN-Verbindung an.

Werkseinstellung

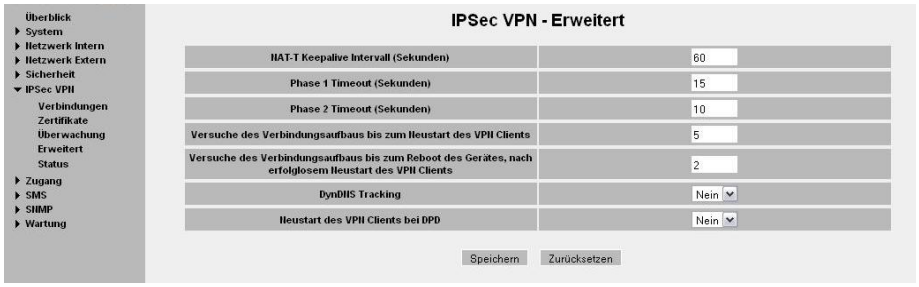
Werkseitig verwendet das TAINY xMOD-V2-IO folgende Einstellungen:

VPN-Überwachung verwenden	**Nein**
Intervall für Verbindungsprüfung (Minuten)	**5**
Verzögerung bis zur Wiederholung (Minuten)	**1**
Anzahl der Wiederholungen	**3**

7.7 Erweiterte Einstellungen bei VPN-Verbindungen

IPsec-VPN > Erweitert

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO



Funktion	Einstellen spezieller Wartezeiten und Intervalle bei VPN-Verbindungen.
NAT-T Keepalive Intervall (Sekunden)	Ist NAT-T aktiviert (vgl. Kapitel 7.3) dann werden periodisch Keepalive-Datenpakete vom TAINY xMOD-V2-IO durch die VPN-Verbindung gesendet. Dies soll verhindern, dass ein NAT-Router zwischen TAINY xMOD-V2-IO und der Gegenstelle in Ruhephasen ohne Datenverkehr, die Verbindung unterbricht. Das Intervall zwischen den Keepalive-Datenpaketen können Sie hier ändern.
Phase 1 Timeout (Sekunden)	Das Phase 1 Timeout bestimmt, wie lange das TAINY xMOD-V2-IO abwartet, bis ein Authentifizierungsverfahren der ISAKMP-SA abgeschlossen ist. Wird das eingestellte Timeout überschritten, wird das Authentifizierungsverfahren abgebrochen und neu gestartet. Das Timeout können Sie hier ändern.
Phase 2 Timeout (Sekunden)	Das Phase 2 Timeout bestimmt, wie lange das TAINY xMOD-V2-IO abwartet, bis ein Authentifizierungsverfahren der IPsec-SA abgeschlossen ist. Wird das eingestellte Timeout überschritten, wird das Authentifizierungsverfahren abgebrochen und neu gestartet. Das Timeout können Sie hier ändern.
Versuche des Verbindungsaufbaus bis Neustart des VPN-Clients	Schlägt ein VPN-Verbindungsaufbau fehl, wird der Verbindungsaufbau vom TAINY xMOD-V2-IO wiederholt. Geben Sie hier die Anzahl der erfolglosen Versuche ein, bevor das TAINY xMOD-V2-IO seinen VPN-Client neu startet um dann erneut den Verbindungsaufbau einzuleiten.
Versuche des Verbindungsaufbaus bis Reboot des Gerätes, nach erfolglosem Neustart des VPN-Clients	Schlägt nach dem Neustart des VPN-Clients der VPN-Verbindungsaufbau fehl, wird der Verbindungsaufbau vom TAINY xMOD-V2-IO wiederholt. Geben Sie hier die Anzahl der erfolglosen Versuche ein, bevor das TAINY xMOD-V2-IO einen Reboot durchführt, um dann erneut den VPN-Verbindungsaufbau einzuleiten.
DynDNS Tracking	Bezieht das VPN-Gateway der Gegenstelle die IP-Adresse von einem DynDNS-Dienst und wird keine Dead Peer Detection verwendet, ist es sinnvoll, dass das TAINY xMOD-V2-IO regelmäßig überprüft, of das VPN-Gateway der Gegenstelle noch erreichbar ist. Das DynDNS Tracking übernimmt diese Funktion. Mit Ja, wird die Funktion aktiviert, mit Nein deaktiviert.
DynDNS Tracking Intervall (Minuten)	Stellen Sie hier ein, in welchen Abständen per DynDNS Tracking geprüft werden soll, ob die Gegenstelle noch erreichbar ist.
Werkseinstellung	Werkseitig verwendet das TAINY xMOD-V2-IO folgende Einstellungen:

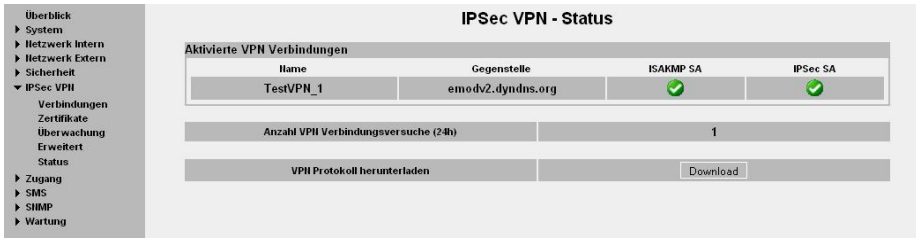
NAT-T Keepalive Intervall (Sekunden)	**60**
Phase 1 Timeout (Sekunden)	**15**
Phase 2 Timeout (Sekunden)	**10**

Versuche des Verbindungsaufbaus bis Neustart des VPN-Clients	**5**
Versuche des Verbindungsaufbaus bis Reboot des Gerätes, nach erfolglosem zum Neustart des VPN-Clients	**2**
DyNDNS Tracking	**Nein**
DynDNS Tracking Intervall (Minuten)	**5**
Neustart des VPN-Clients bei DPD	**Nein**

7.8 Status der VPN-Verbindungen

IPsec-VPN > Status

NUR TAINY HMOD-V2-IO
NUR TAINY EMOD-V2-IO

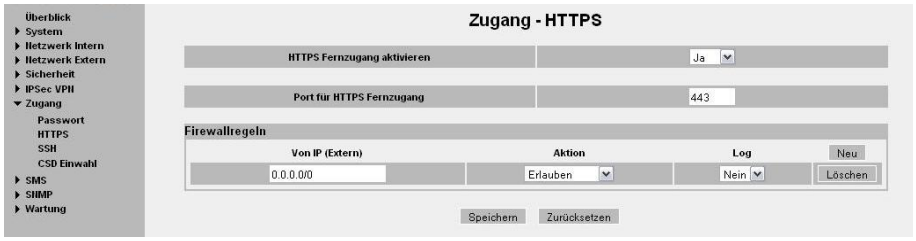


Funktion	Anzeige des Status der aktivierten VPN-Verbindungen und Möglichkeit eine Protokolldatei auf den Admin-PC zu laden.
Aktivierte VPN-Verbindungen	Die jeweilige Sicherheitsbeziehung (SA = Security Association) ist erfolgreich aufgebaut. Die Sicherheitsbeziehung besteht nicht.
Anzahl VPN-Verbindungsversuche (24h)	Zeigt die Anzahl der Versuche seit 0:00 Uhr (Systemzeit) an, die aktivierten VPN-Verbindungen aufzubauen.
VPN Protokoll herunterladen	Mit dieser Funktion können Sie die VPN-Protokolldatei auf den Admin-PC herunterladen.

8 Fernzugänge

8.1 Fernzugang HTTPS

Zugang > HTTPS



Funktion

Der HTTPS-Fernzugang (= *HyperText Transfer Protocol Secure*) ermöglicht über HSDPA, UMTS, EGPRS oder GPRS einen gesicherten Zugriff aus einem externen Netz auf die Web-Oberfläche des TAINY xMOD.

Die Konfiguration des TAINY xMOD über den HTTPS-Fernzugang erfolgt dann genauso wie die Konfiguration per Web-Browser über die lokale Schnittstelle.

HTTPS Fernzugang aktivieren

Ja — Der Zugriff auf die Web-Oberfläche des TAINY xMOD per HTTPS aus dem externen Netz ist gestattet.

Nein — Der Zugriff per HTTPS ist nicht gestattet.

Port für HTTPS Fernzugang

Standard: 443 (Werkseinstellung)

Sie können hier einen alternative Port festlegen. Wenn Sie den alternativen Port nutzen wollen, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe vor der IP-Adresse die Nummer des alternativen Ports angeben.

Beispiel:
Ist dieses TAINY xMOD über die Adresse 192.144.112.5 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 442 festgelegt, dann muss bei der externen Gegenstelle im Web-Browser angegeben werden:
https://192.144.112.5:442

Hinweis

Der Standard-Port 443 für den HTTPS-Zugang bleibt neben dem neu gewählten Port offen.

Firewall-Regeln für den HTTPS-Fernzugang

Neu — Fügt eine neue Firewall-Regel für den HTTPS-Fernzugang hinzu, die Sie dann ausfüllen können.

Löschen — Entfernt eine angelegte Firewall-Regel für den HTTPS-Fernzugang wieder.

Von IP (extern) — Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse oder -Adressenbereich: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

Aktion Bestimmen Sie wie bei Zugriffen auf den angegebenen HTTPS-Port verfahren wird:

Erlauben bedeutet, die Datenpakete dürfen passieren.

Zurückweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.

Log Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen,
oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4, geschrieben.

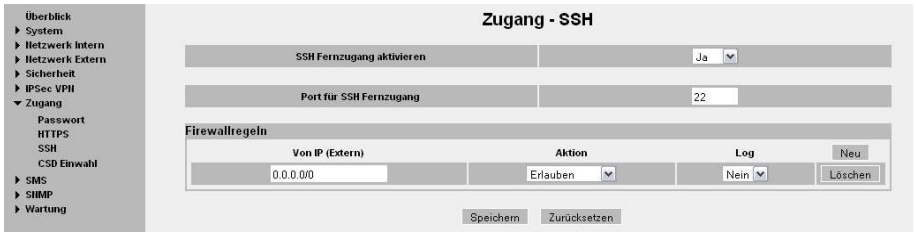
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

HTTPS Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für HTTPS Fernzugang	**443**
Vorgabe für neue Regel:	
Von IP (extern)	**0.0.0.0/0**
Aktion	**Erlauben**
Log	**Nein (Ausgeschaltet)**

8.2 Fernzugang – SSH

Zugang > SSH



Funktion

Der SSH-Fernzugang (= *Secured SHell*) ermöglicht über HSDPA, UMTS, EGPRS oder GPRS einen gesicherten Zugriff aus einem externen Netz auf das Dateisystem des TAINY xMOD.

Dazu muss mit einem SSH-fähigen Programm eine Verbindung von der externen Gegenstelle zum TAINY xMOD aufgebaut werden.

Verwenden Sie den SSH-Fernzugang nur, wenn Sie mit dem LINUX-Dateisystem vertraut sind.

Werkseitig ist diese Option ausgeschaltet.

Vorsicht

Über den SSH-Fernzugang ist es möglich, das Gerät so falsch zu konfigurieren, dass es zum Service eingeschickt werden muss. Kontaktieren Sie in diesem Fall bitte Ihren Händler oder Distributor.

SSH-Fernzugang aktivieren

Ja Der Zugriff auf das Dateisystem des TAINY xMOD per SSH aus dem externen Netz ist gestattet.

Nein Der Zugriff per SSH ist nicht gestattet.

Port für SSH-Fernzugang

Standard: 22 (Werkseinstellung)

Sie können hier einen alternative Port festlegen. Wenn Sie den alternativen Port nutzen wollen, dann muss die externe Gegenstelle, die den Fernzugriff ausübt, bei der Adressenangabe vor der IP-Adresse die Nummer des alternativen Ports angeben.

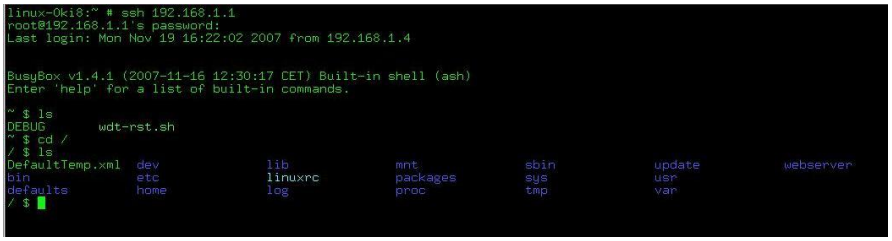
Hinweis

Der Standard-Port 22 für den SSH Zugang bleibt neben dem neu gewählten Port offen.

Beispiel:
Ist dieses TAINY xMOD über die Adresse 192.144.112.5 aus dem externen Netz zu erreichen, und ist für den Fernzugang der Port 22222 festgelegt, dann muss bei der externen Gegenstelle im SSH-Client (z. B. PUTTY) diese Port-Nummer angegeben werden:

ssh -p 22222 192.144.112.5

Beispiel Konsole:


linux-Oki8:~ # ssh 192.168.1.1
root@192.168.1.1's password:
Last login: Mon Nov 19 16:22:02 2007 from 192.168.1.4
BusyBox v1.4.1 (2007-11-16 12:30:17 CET) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
~ $ ls
DEBUG wdt-rst.sh
~ $ cd /
/ $ ls
DefaultTemp.xml dev lib mnt sbin update webserver
bin etc linuxrc packages sys usr
defaults home log proc tmp var
/ $

Firewall-Regeln für den SSH-Fernzugang

Neu — Fügt eine neue Firewall-Regel für den SSH-Fernzugang hinzu, die Sie dann ausfüllen können.

Löschen — Entfernt eine angelegte Firewall-Regel für den SSH-Fernzugang wieder.

Von IP (extern) — Geben Sie hier die Adresse(n) des/der Rechner(s) an, dem/denen Fernzugang erlaubt ist. Bei den Angaben haben Sie folgende Möglichkeiten:

IP-Adresse oder -Adressenbereich: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

Aktion — Bestimmen Sie wie bei Zugriffen auf den angegebenen SSH-Port verfahren wird:

Erlauben bedeutet, die Datenpakete dürfen passieren.

Zurückweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verworfen, so dass der Absender keine Information erhält über deren Verbleib.

Log — Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - *Log* auf *Ja* setzen
oder nicht - *Log* auf *Nein* setzen (werkseitige Voreinstellung).

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

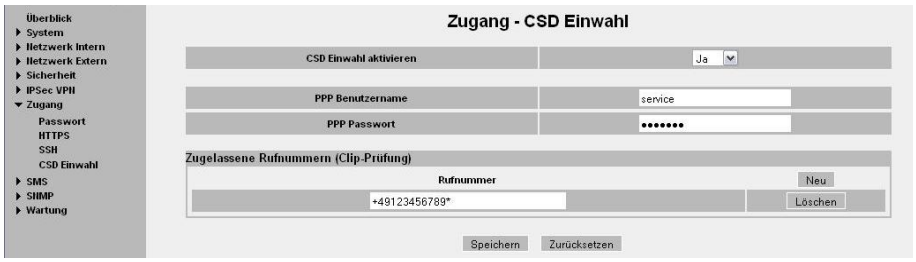
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

SSH Fernzugang aktivieren	**Nein (Ausgeschaltet)**
Port für SSH Fernzugang	**22**
Vorgabe für neue Regel:	
Von IP (extern)	**0.0.0.0/0**
Aktion	**Erlauben**
Log	**Nein (Ausgeschaltet)**

8.3 Fernzugang über Wählverbindung

Zugang > CSD-Einwahl



Funktion

Der Zugang CSD-Einwahl ermöglicht den Zugriff auf die Web-Oberfläche und ssh-Konsole des TAINY xMOD über eine Daten-Wählverbindung (*CSD = Circuit Switched Data*). Rufen Sie dazu das TAINY xMOD mit einem analogen Modem auf der Datenrufnummer oder mit einem GSM-Modem auf der Sprach- oder Datenrufnummer seiner SIM-Karte an. Das TAINY xMOD nimmt den Ruf an, wenn

- die Rufnummer des Telefonanschlusses von dem aus Sie den Anruf tätigen in der Liste der zugelassenen Nummern im TAINY xMOD gespeichert ist und
- die Rufnummer vom Telefonnetz übertragen wird (CLIP-Funktion)

Die Einwahl muss mit einem PPP-Client erfolgen, zum Beispiel über eine Windows DFÜ-Verbindung. Folgen Sie unter Windows dem *Assistenten für neue Verbindungen* und richten Sie als *Verbindung mit dem Netzwerk am Arbeitsplatz* eine *DFÜ-Verbindung* ein.

Web-Oberfläche und ssh-Konsole haben bei CSD-Einwahl die IP-Adresse 10.99.99.1.

NUR für TAINY HMOD

Hinweis

Beim TAINY HMOD ist diese Funktion nur verfügbar, wenn ein GSM-Netz verwendet wird. In UMTS-Netzen, kann diese Funktion nicht verwendet werden.

CSD-Einwahl aktivieren

Ja	Der Zugriff auf die Web-Oberfläche des TAINY xMOD per Daten-Wählverbindung ist gestattet.
Nein	Der Zugriff per Daten-Wählverbindung ist nicht gestattet.

PPP Benutzername / Passwort

Wählen Sie einen Benutzernamen und ein Passwort aus, mit dem sich ein PPP-Client (z.B. Windows DFÜ-Verbindung) am TAINY xMOD anmelden muss. Den gleichen Benutzernamen und das gleiche Passwort müssen Sie beim PPP-Client eintragen.

Zugelassene Rufnummern

Geben Sie die Rufnummer des Telefonanschlusses an, von dem aus die Daten-Wählverbindung aufgebaut wird. Der Telefonanschluss muss die Rufnummernübermittlung (CLIP – Calling Line Identification Presentation) unterstützen und die Funktion muss eingeschaltet sein.

Die im TAINY xMOD eingetragene Rufnummer muss exakt mit der gemeldeten Rufnummer übereinstimmen und gegebenenfalls auch die Länderkennung und Vorwahl umfassen, z.B. +494012345678.

Wenn mehrere Rufnummern einer Nebenstellenanlage zugangsberechtigt sein sollen, können sie das Zeichen „*“ als Joker verwenden, z.B. +49401234*. Alle Rufnummern die mit +49401234 beginnen werden dann akzeptiert.

Hinweis

Firewall-Regeln, die für den HTTPS- bzw. SSH-Zugang eingetragen sind, gelten auch für den CSD-Zugang. Als Quell-IP-Adresse („*von IP*“) für den CSD-Zugang ist 10.99.99.2 festgelegt.

Neu Fügt eine neue zugelassene Rufnummer für den CSD-Fernzugang hinzu, die Sie dann ausfüllen können.

Löschen Entfernt eine Rufnummer für den CSD-Fernzugang wieder.

Werkseinstellung

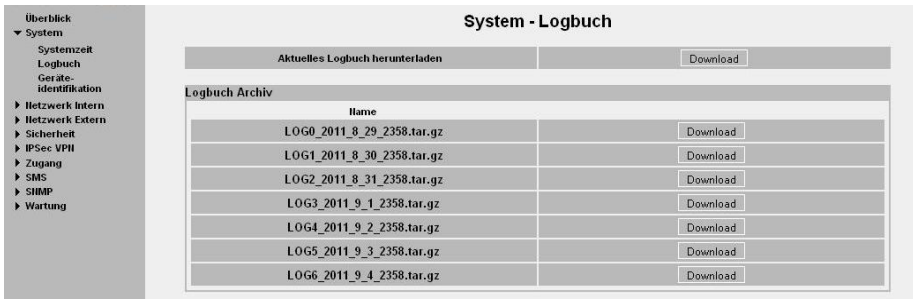
Werkseitig hat das TAINY xMOD folgende Einstellungen:

CSD-Einwahl aktivieren	**Nein (Ausgeschaltet)**
PPP Benutzername	**service**
PPP Passwort	**service**
Zugelassene Rufnummern	*****

9 Logbuch, Update und Diagnose

9.1 Anzeige Logbuch

System > Logbuch



Logbuch

Im Logbuch werden wichtige Ereignisse im Betriebsablauf des TAINY xMOD abgespeichert:

- Neustart
- Änderungen der Konfiguration
- Verbindungsaufbau
- Verbindungsunterbrechungen
- Signalstärke
- u.v.m.

Das Logbuch wird bei Erreichen einer Dateigröße von 1MByte, spätestens aber nach 24 Stunden im Logbuch Archiv des TAINY xMOD gespeichert.

Aktuelles Logbuch herunterladen

Download - das aktuelle Logbuch wird auf den Admin-PC geladen. Sie können das Verzeichnis auswählen, in dem die Datei dort gespeichert wird und die Datei dort betrachten.

Logbuch Archiv

Download - archivierte Logbuch-Dateien werden auf den Admin-PC geladen. Sie können das Verzeichnis auswählen, in dem die Dateien dort gespeichert werden und die Dateien dort betrachten.

Beispiel:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
13.12.2007 11:04	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
13.12.2007 19:46	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
13.12.2007 19:47	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
13.12.2007 20:03	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:19	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:36	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 20:52	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
13.12.2007 21:25	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:	RXS:	TX:0	RX:0;
14.12.2007 12:15	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.IP:192.168.1.1					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_0.NetMask:255.255.255.0					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.IP:192.168.0.20					
14.12.2007 12:16	3173XX	CSQ=---	STAT=---	COPS=---	(null)	4	CH	9	CONFIGURATION FILE ACCESS	InternalIPs.InternalIP_1.NetMask:255.255.255.0					
14.12.2007 23:05	3173XX	(null)	(null)	(null)	SERVICE_MASK=0	4	UH	41	CURRENT SYSTEM VERSION	1.014					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	SERVICE_MASK=495591	4	APL	0	SYSTEM STARTING	Success					
14.12.2007 23:05	3173XX	CSQ=---	STAT=---	COPS=---	(null)	0	APL	5	CONNECTION ERROR	Missing or incorrect GSM parameter					
14.12.2007 23:08	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:09	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	3	GPRS CONNECTION ESTABLISHED	GPRS connect					
14.12.2007 23:10	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	APL	8	IP ASSIGNED	172.25.105.9					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495591	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:11	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:12	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	ICMPCheck.Enabled:true					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	(write values)					
14.12.2007 23:13	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=495615	4	CH	9	CONFIGURATION FILE ACCESS	NTP.Enabled:true					
14.12.2007 22:24	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:40	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 22:57	3173XX	CSQ=8	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:13	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:449	RXS:358	TX:1078	RX:358;
14.12.2007 23:30	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:2737	RXS:3931	TX:3366	RX:3931;
14.12.2007 23:46	3173XX	CSQ=10	STAT=1	COPS=26201	SERVICE_MASK=499711	4	APL	34	SYSTEM RUNNING SUCCESSFUL	CellID:4389	Version:1.014	TXS:3089	RXS:4469	TX:3718	RX:4469;

Einträge im Logbuch

Spalte A: Zeitstempel

Spalte B: Dr. Neuhaus Produktnummer

Spalte C: Signalqualität (CSQ-Wert)

Spalte D: GSM-Einbuchstatus

STAT = --- = Funktion noch nicht gestartet

STAT = 1 = Im Heimatnetz eingebucht

STAT = 2 = Nicht eingebucht; Netzsuche

STAT = 3 = Einbuchen abgelehnt

STAT = 5 = Eingebucht in Fremdnetz (Roaming)

Spalte E: Angabe der Identifikation des Netzbetreibers mit dem 3-stelligen Ländercode (MCC) und dem 2-3-stelligen Netzbetreibercode (MNC).

Beispiel: 26201 (262 = Ländercode / 01 = Netzbetreibercode)

Spalte F: Kodierter Betriebsstatus (für Kundendienst)

Spalte G: Kategorie des Logbuch-Meldung (für Kundendienst)

Spalte H: Interne Quelle des Logbuch-Meldung (für Kundendienst)

Spalte I: Interne Meldungsnummer (für Kundendienst)

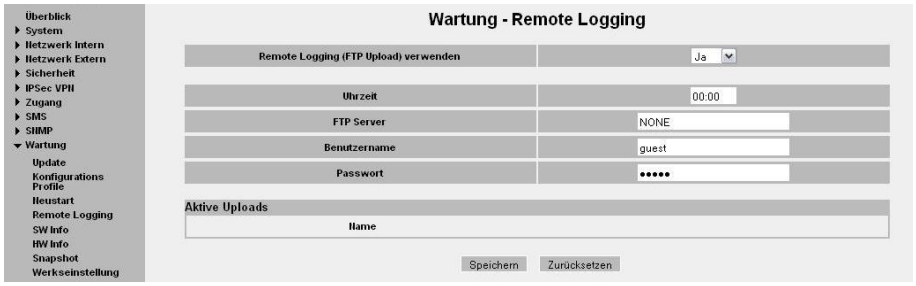
Spalte J: Logbuch-Meldung im Klartext

Spalten K-P: Zusatzinfomationen zur Klartextmeldung, wie zum Beispiel:

- Cell-ID (Identifikationsnummer der aktiven GSM-Zelle)
- Softwareversion
- TXS, RXS (Übertragene IP-Pakete der aktuellen Verbindung)
- TX, RX (Übertragene IP-Pakete seit letztem Werksneustart)

9.2 Remote Logging

Wartung > Remote Logging



Funktion

Das TAINY xMOD kann das System-Logbuch einmal am Tag per FTP (= File Transfer Protocol) an einen FTP-Server übertragen.

Übertragen wird das aktuelle System-Logbuch sowie die System-Log-Dateien im Archiv. Nach erfolgreicher Übertragung werden die übertragenen System Logbücher im TAINY xMOD gelöscht.

Schlägt die Übertragung fehl, versucht das TAINY xMOD nach 24 Stunden erneut die Daten zu übertragen.

Hinweis

Nach fehlgeschlagenem FTP-Upload werden die Logfiles unter Wartung > Remote Logging abgelegt.

Remote Logging (FTP Upload) verwenden	Mit *Ja* wird die Funktion eingeschaltet.
Uhrzeit	Legt die *Uhrzeit* fest, zu der die Logbücher übertragen werden sollen.
FTP-Server	Legt die Adresse des *FTP-Servers* fest, zu dem die Log-Dateien übertragen werden sollen. Die Adresse kann als Hostname (z.B. ftp.server.de) oder als IP-Adresse angegeben werden.
Benutzername	Legt den Benutzernamen für die Anmeldung am FTP-Server fest.
Passwort	Legt das Passwort für die Anmeldung am FTP-Server fest.

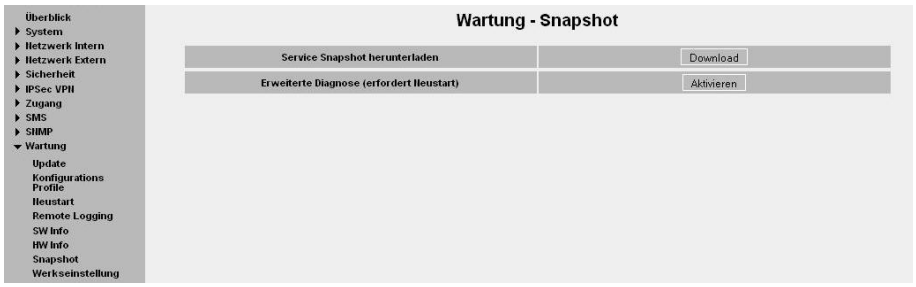
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Remote Logging (FTP Upload) verwenden	**Nein (Ausgeschaltet)**
Uhrzeit	**00:00**
FTP-Server	**NONE**
Benutzername	**guest**
Passwort	**Guest**

9.3 Snapshot

Wartung > Snapshot



Funktion	Diese Funktion dient für Support-Zwecke. Der Service-Snapshot speichert wichtige Logdateien und aktuelle Geräte-Einstellungen, die zur Fehlerdiagnose relevant sein könnten in einer Datei. Wenn Sie sich bei einem Problem mit dem TAINY xMOD an unseren Kundendienst wenden, wird dieser in vielen Fällen um die Snapshot-Datei bitten.

Hinweis

Diese Datei enthält die Zugangsparameter zum Datenfunkdienst (HSDPA, UMTS, EGPRS oder GPRS) sowie die Adressen der Gegenstelle. Nicht enthalten sind Benutzername und Passwort für den Zugang zum TAINY xMOD.

Service Snapshot herunterladen	Klicken Sie auf Download. Sie können auswählen, an welche Stelle auf dem Admin-PC die Snapshot-Datei gespeichert werden soll. Der Dateiname der Snapshot-Datei setzt sich folgendermaßen zusammen: <hostname>_Snapshot_<Date&TimeCode>.tgz, z.B.: tainyHMOD_Snapshot_200711252237.tgz

Erweiterte Diagnose

Aktivieren Sie bitte die *erweiterte Diagnose* nur nach Aufforderung durch unseren Kundendienst. Im Betrieb werden bei erweiterter Diagnose viel häufiger Informationen in die Diagnose-Logbücher geschrieben. Es werden auch zusätzliche Informationen gespeichert. Dies hilft bei einer gezielten Problemanalyse.

Hinweis

Durch die häufigen Schreibzugriffe bei aktivierter erweiterter Diagnose auf den nicht-flüchtigen Speicher des TAINY xMOD kann sich dessen Lebensdauer verringern.

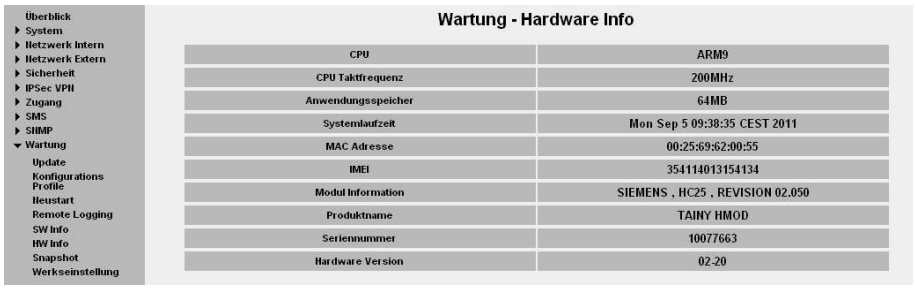
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

Erweiterte Diagnose	**Aus (Aktivieren)**

9.4 Hardware Informationen

Wartung > Hardware Info

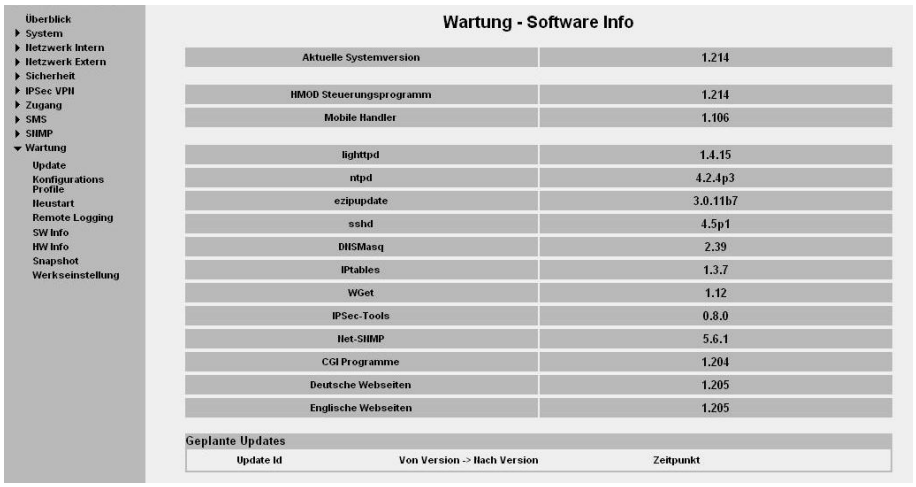


Funktion

Anzeige wichtiger Informationen zur Hardware-Identifikation. Bei Anfragen an unseren Kundendienst werden diese Informationen in vielen Fällen benötigt.

9.5 Software Informationen

Wartung > Software Info



Funktion

Anzeige wichtiger Informationen zur SoftwareIdentifikation. Bei Anfragen an unseren Kundendienst werden diese Informationen in vielen Fällen benötigt.

Zusätzlich werden geplante Updates angezeigt. Siehe auch Kapitel 9.6.

9.6 Software Update

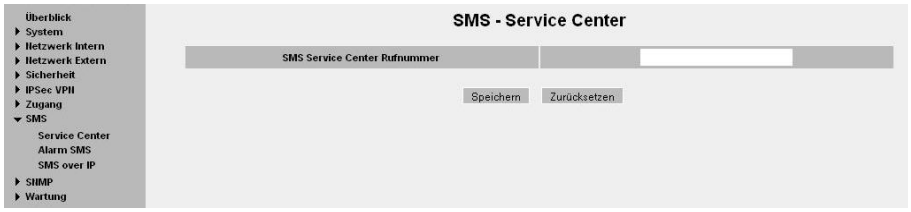
Wartung > Update

Funktion	Mit der Update Funktion können Sie eine neue Betriebssoftware in das TAINY xMOD laden und diese Software aktivieren. Bei einem sofortigen Update wird die neue Software entpackt. Dieser Vorgang kann einige Minuten dauern. Danach beginnt der eigentliche Update-Vorgang, der durch ein Lauflicht der LEDs angezeigt wird. Die Einstellungen des TAINY xMOD werden übernommen, sofern diese Einstellungen in der neuen Software-Version noch so wirken, wie vor dem Update.	
Zeitpunkt festlegen	*Nein*	Update sofort - Die neue Betriebssoftware wird aktiviert, direkt nachdem Sie die Software geladen und auf die Schaltfläche *Absenden* geklickt haben.
	Ja	Update zeitgesteuert - Die neue Betriebssoftware wird aktiviert, an dem festgelegten Update Zeitpunkt. Dazu muss die Software zuvor geladen werden.
Update Zeitpunkt festlegen	Wenn Sie das Update zeitgesteuert durchführen lassen wollen, geben Sie den Zeitpunkt an, an dem die neue Betriebssoftware aktiviert werden soll. Geben Sie Jahr – Monat – Tag – Stunde – Minute an.	
Update Datei auswählen	Wählen Sie mit *Durchsuchen* die neue Betriebsssoftware aus. Die Betriebssoftware für das TAINY xMOD trägt zum Beispiel folgende Bezeichnung: HMOD_V2IO_v1.107-v1.214.tgz Laden Sie die Firmware mit *Öffnen* in das Gerät.	
Absenden	Mit *Absenden* wird die Betriebssoftware entweder sofort aktiviert oder die Betriebssofware wird zum vorgegeben Zeitpunkt aktiviert.	

10 SMS-Versand

10.1 Service Center

TAINY xMOD nutzt auch den Short Message Service (SMS) von GSM. Sie können ein spezielles SMS-Center festlegen.



SMS Service Center Rufnummer

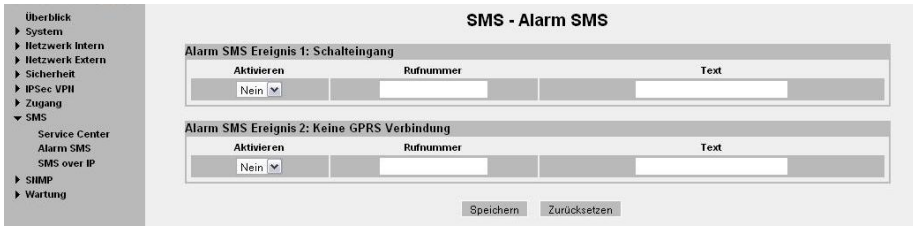
Damit die SMS-Funktion sicher funktioniert, tragen Sie hier die Rufnummer des Service Center ein. Ohne Eintrag an dieser Stelle wird das Standard SMS Service Center Ihres Netzbetreibers verwendet. Durch das Fehlen des Eintrags kann es zu Fehlfunktionen kommen.

Achtung:

Wird keine Rufnummer für das SMS-Center eingetragen, oder erfolgt der Eintrag nicht in internationalem Format (z.B. +49…) kann der SMS-Versand scheitern.

10.2 Alarm SMS

SMS > Alarm SMS



Funktion

Das TAINY xMOD kann kurze Alarm-Meldungen über SMS (= Short Message Service) des GSM-Netzes versenden. Zwei Ereignisse können den Versand einer Alarm-Meldung über SMS auslösen:

- Ereignis 1: Schalteingang wird aktiv
- Ereignis 2: Keine UMTS- bzw. GPRS-Verbindung

Zu jedem der beiden Ereignisse kann eine eigene Rufnummer angegeben werden, an die die Alarm-Meldung geschickt wird. Ebenso kann der Text der Alarm-Meldung frei festgelegt werden. Es stehen folgende Zeichen zur Verfügung: A-Z a-z 0123456789,!?

Alarm SMS Ereignis 1: Schalteingang

Ereignis 1: der Schalteingang wechselt von inaktiv auf aktiv, d.h. am Schalteingang wird eine ausreichende Schaltspannung angelegt. Diese Funktion kann zum Beispiel genutzt werden, um außerhalb der IP-Datenverbindungen Alarm-Meldungen der lokalen Applikationen zu versenden.

Alarm SMS Ereignis 2: Keine GPRS-Verbindung

Ereignis 2: die Verbindung zum Datenfunkdienst (HSDPA, UMTS, EGPRS, GPRS) kommt trotz mehrfacher Versuche nicht zustanden. TAINY xMOD versendet daraufhin eine Alarm-Meldung.

Einstellungen

Aktivieren Bei *Ja* wird bei dem Ereignis die Alarm-Meldung abgesendet, bei *Nein* nicht.

Rufnummer Tragen Sie hier die Rufnummer des Endgerätes ein, an die die Alarm-Meldung über SMS gesendet werden soll. Das Endgerät muss SMS-Empfang über GSM oder Festnetz unterstützen.

Text Tragen Sie hier den Text ein, der als Alarm-Meldung verschickt wird.

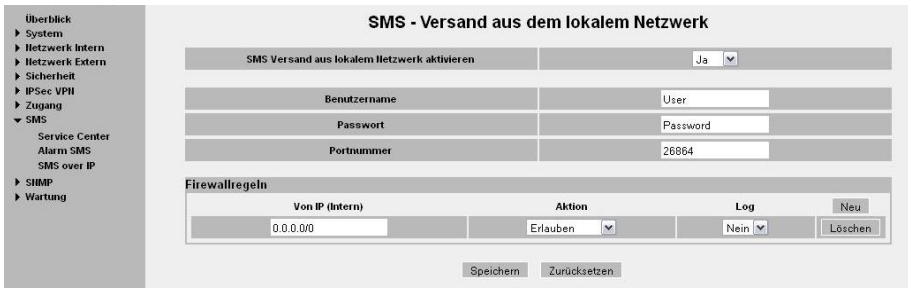
Werkseinstellung

Werkseitig hat das TAINY xMOD folgende Einstellungen:

SMS Service Center Rufnummer	**-**
Alarm SMS Ereignis 1: Schalteingang	**Nein (Ausgeschaltet)**
Rufnummer	**-**
Text	**-**
Alarm SMS Ereignis 2: : Keine GPRS-Verbindung	**Nein (Ausgeschaltet)**
Rufnummer	**-**
Text	**-**

10.3 SMS-Versand aus dem lokalem Netzwerk

SMS – Versand aus dem lokalen Netzwerk



Mit der Funktion SMS-Versand können Anwendungen, die an der lokalen Schnittstelle des TAINY xMOD angeschlossen sind, über das GSM-Netz Short Messages (SMS) verschicken.

Zum Versand einer SMS muss die Anwendung an der lokalen Schnittstelle eine TCP/IP-Verbindung zum TAINY xMOD aufbauen.

Über diese TCP/IP-Verbindung sendet die Anwendung den Text der SMS an das TAINY xMOD, welches den Text in eine SMS verpackt und diese verschickt.

Rahmen auf der TCP/IP-Verbindung

Der Text muss in folgendem Rahmen über die TCP/IP-Verbindung an das TAINY xMOD übermittelt werden:

Benutzername#Passwort#CommandCode#Seq-Num;Rufnummer;Nachricht:

Beispiel: benutzer#passwort#105#01;0049043465789;Mein SMS-Text:

Benutzername

Der Benutzername zur Prüfung der Berechtigung zum Senden einer SMS. Maximal dürfen 10 Zeichen verwendet werden.

Passwort

Das Passwort zur Prüfung der Berechtigung zum Senden einer SMS. Maximal dürfen 10 Zeichen verwendet werden.

CommandCode

Kommando zum SMS-Versand aus dem lokalen Netz. Dieser Wert ist fest 105 und darf nicht verändert werden.

Seq-Num

Die Sequenznummer dient der Zuordnung mehrerer Anfragen gleichzeitig. Die Funktion wird derzeit nicht unterstützt.

Die Sequenznummer besteht aus 2 numerischen Zeichen zwischen 01 bis 99

Rufnummer

Rufnummer des SMS-Empfängers. Die Rufnummer darf 40 Zeichen nicht übersteigen. Internationale Nummern (+49..) sind zulässig.

Nachricht

SMS Text. Der Text darf 160 Zeichen nicht übersteigen.

Es stehen folgende Zeichen zur Verfügung: A-Z a-z 0123456789,!?

Folgende Zeichen haben eine besondere Bedeutung und dürfen im SMS-Text nicht vorkommen:

#	Trennungszeichen der ersten Kommandoebene
;	Trennungszeichen der zweiten Kommandoebene
:	Bestimmt das Ende der Nachricht

SMS-Versand aus dem lokalen Netzwerk aktivieren	Wählen Sie Ja um SMS aus dem lokalen Netzwerk versenden zu können.
Benutzername	Benutzername, der im Nachrichten-Rahmen enthalten sein muss, bevor deren Text per SMS versendet wird. Maximal dürfen 10 Zeichen verwendet werden.
Passwort	Passwort, das im Nachrichten-Rahmen enthalten sein muss, bevor deren Text per SMS versendet wird. Maximal dürfen 10 Zeichen verwendet werden.
Portnummer	TCP/IP-Port auf dem das TAINY xMOD die TCP/IP-Verbindung zum SMS-Versand entgegen nimmt.
Firewall-Regeln	Damit die TCP/IP-Verbindung zum SMS-Versand aufgebaut werden kann, muss am TAINY xMOD eine Firewall-Regel eingerichtet werden. Es können mit Neu mehrere Quellen (Von IP) für die TCP/IP-Verbindung zum SMS-Versand eingerichtet werden. Mit Löschen können Sie Verbindungen wieder entfernen.

Von IP

Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. 0.0.0.0/0 bedeutet alle Adressen.

Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12.

Aktionen

Wählen Sie Aktionen, um die TCP/IP-Verbindung zum SMS-Versand zu erlauben.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

das Ereignis protokolliert werden soll - Log auf Ja setzen

oder nicht - Log auf Nein setzen (werkseitige Voreinstellung)

Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Werkseinstellung

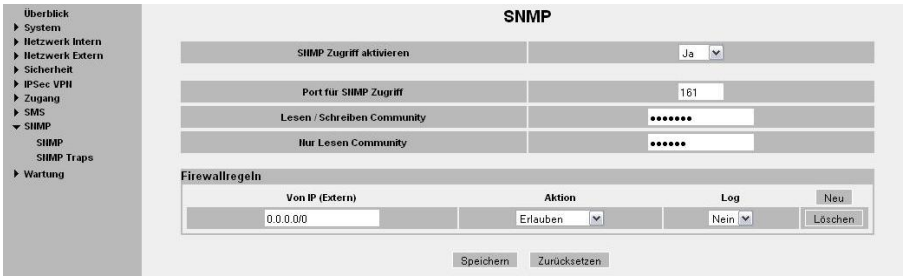
Werkseitig hat das TAINY xMOD folgende Einstellungen:

Benutzername	User
Passwort	Password
Portnummer	26864
Firewall-Regeln	Nicht aktiv
Von IP	0.0.0.0/0
Aktionen	Erlauben
Log	Nein

11 SNMP

11.1 Bedienung per SNMP

SNMP – SNMP



Verschiedene Parameter des TAINY xMOD können Mithilfe des SNMP Version 1 und Version 2 (Simple Network Management Protocol) abgefragt oder geändert werden.

Der Zugriff per SNMP kann sowohl aus dem lokalen Netz als auch vom externen Netz erfolgen.

Folgende SNMP-Anfragen und -Antworten werden vom TAINY xMOD unterstützt:

GET, GETNEXT, GETBULK, GETSUBTREE, WALK, SET, RESPONSE, TRAP.

Auf die folgenden Parameter des TAINY xMOD kann per SNMP lesend zugegriffen werden:

- Geräteidentifikations-Zeilen (1-4)
- IP-Adresse des externen Netzwerks
- PIN
- MAC-Adresse der lokalen Schnittstelle
- Kennung des aktuellen Mobilfunkbetreibers
- APN
- IMSI
- IMEI
- Signalqualität (CSQ-Wert)
- Cell-ID
- Cell-IDs der Nachbarzellen
- Hostname
- Maximales Datenvolumen
- Datenvolumen der Warnschwelle 80%
- Aktuell verbrauchtes Datenvolumen (Monatsvolumen)
- Hardware-ID
- Softwareversion
- Versionsnummer des integrierten Funkmoduls

Folgende Parameter des TAINY xMOD können per SNMP verändert werden:

- Maximales Datenvolumen (Volumenbegrenzung)
- PIN der SIM-Karte
- Geräteidentifikations-Zeilen (1-4)

Die exakte Beschreibung der Parameter wird als MIB (Management Information Base) auf der Dr. Neuhaus Webseite www.neuhaus.de zur Verfügung gestellt. Gehen Sie dort zur Produktseite des TAINY xMOD.

SNMP-Zugriff aktivieren	Wählen Sie *Nein*, wenn Sie den SNMP-Zugriff auf das TAINY xMOD sperren wollen. Wählen Sie *Ja*, wenn Sie den SNMP-Zugriff auf das TAINY xMOD zulassen wollen.
Port für SNMP Zugriff	Wählen sie den IP-Port aus, über den der SNMP Zugriff erfolgen soll. Die Werkseinstellung entspricht dem Standard (Port 161).
Lesen / Schreiben Community	Geben Sie die SNMP-Community ein, die lesend und schreibend auf das TAINY xMOD zugreifen darf.
Nur Lesen Community	Geben Sie die SNMP-Community ein, die nur lesend auf das TAINY xMOD zugreifen darf.
Firewall-Regeln	Damit Daten per SNMP ausgetauscht werden können, muss am TAINY xMOD eine Firewall-Regel eingerichtet werden. Es können mit Neu mehrere Quellen (Von IP) für die UDP/IP-Verbindung eingerichtet werden. Mit Löschen können Sie Verbindungen wieder entfernen. **Von IP** Tragen Sie die IP-Adresse der externen Gegenstelle ein, die IP-Pakete zum lokalen Netz senden darf. Geben Sie dazu die IP-Adresse oder einen IP-Bereich der Gegenstelle an. 0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe Kapitel 12. **Aktionen** Wählen Sie Aktionen, um die UDP/IP-Verbindung für SNMP zu erlauben. **Log** Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel das Ereignis protokolliert werden soll - Log auf Ja setzen oder nicht - Log auf Nein setzen (werkseitige Voreinstellung) Das Protokoll wird in das Firewall-Logbuch, siehe Kapitel 6.4 geschrieben.

Werkseinstellung

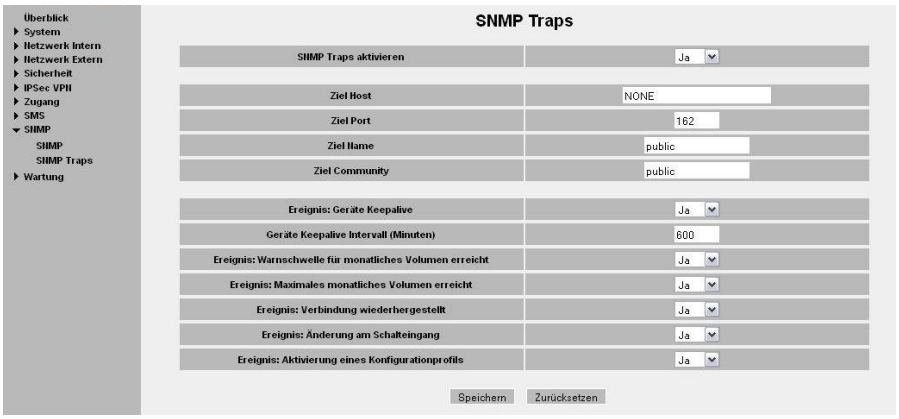
Werkseitig hat das TAINY xMOD folgende Einstellungen:

SNMP Zugriff aktivieren	Nein
Port für SNMP Zugriff	161
Lesen / Schreiben Community	public
Nur Lesen Community	public
Firewall-Regeln	Nicht aktiv
Von IP	0.0.0.0/0

Aktionen	Erlauben
Log	Nein

11.2 Alarmmeldungen per SNMP-Traps

SNMP – SNMP-Traps



Das TAINY xMOD versendet Benachrichtigungen in Form von SNMP-Traps bei verschiedenen Ereignissen.

SNMP-Traps aktivieren	Wählen Sie *Ja*, wenn Sie das Versenden von SNMP-Traps aktivieren wollen. Wählen Sie *Nein*, wenn Sie das Versenden von SNMP-Traps ausschalten wollen.
Ziel Host	Tragen Sie hier die IP-Adresse des SNMP-Trap-Empfängers ein.
Ziel Port	Tragen Sie hier den IP Port des SNMP-Trap-Empfängers ein.
Ziel Name	Tragen Sie hier den Namen des SNMP-Trap-Empfängers ein.
Ziel Community	Tragen Sie hier die Bezeichnung der SNMP-Community ein.
Ereignis: Geräte Keepalive	Wählen Sie *Ja*, wenn das TAINY xMOD Keepalive-Pakete als SNMP-Trap versenden soll. Wählen Sie *Nein*, wenn das TAINY xMOD Keepalive-Pakete als SNMP-Trap nicht versenden soll.
Geräte Keepalive Intervall (Minuten)	Wählen Sie das Intervall mit den die Keepalive SNMP-Traps verschickt werden sollen.
Ereignis: Warnschwelle für monatliches Volumen erreicht	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei Erreichen der Warnschwelle (80%) für das monatliche Datenvolumen versenden soll (siehe Kapitel 5.7). Wählen Sie *Nein*, wenn keinen SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: Maximales monatliches Volumen erreicht	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei Erreichen des maximalen monatlichen Datenvolumens versenden soll (siehe Kapitel 5.7) Wählen Sie *Nein*, wenn keinen SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: Verbindung wiederhergestellt	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei erfolgreicher Wiederherstellung der Verbindung zum APN versenden soll. Wählen Sie *Nein*, wenn keinen SNMP-Trap bei diesem Ereignis versendet werden soll.

Ereignis: Änderung am Schalteingang	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei einer Änderung am Schalteingang versenden soll. Wählen Sie *Nein*, wenn keinen SNMP-Trap bei diesem Ereignis versendet werden soll.
Ereignis: Aktivierung eines Konfigurations-profils	Wählen Sie *Ja*, wenn das TAINY xMOD einen SNMP-Trap bei der Aktivierung eines Konfigurations-Profils versenden soll. Wählen Sie *Nein*, wenn keinen SNMP-Trap bei diesem Ereignis versendet werden soll.

Werkseinstellung

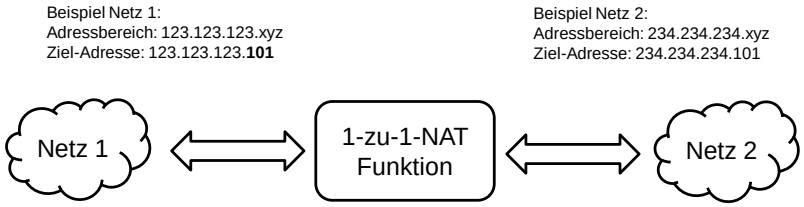
Werkseitig hat das TAINY xMOD folgende Einstellungen:

SNMP-Traps aktivieren	Nein
Ziel Host	NONE
Ziel Port	162
Ziel Name	public
Ziel Community	public
Ereignis: Geräte Keepalive	Ja
Geräte Keepalive Intervall (Minuten)	600
Ereignis: Warnschwelle für monatliches Volumen erreicht	Ja
Ereignis: Maximales monatliches Volumen erreicht	Ja
Ereignis: Verbindung wiederherstellen	Ja
Ereignis: Änderung am Schalteingang	Ja
Ereignis: Aktivierung eines Konfigurations-Profils	Ja

12 Kleines Router-Lexikon

1-zu-1-NAT

Bei 1-zu-1-NAT bildet eine Netzwerkkomponente (z.B.-Router) den Adressbereich des einen Netzes in den Adressbereich eines zweiten Netzes ab.



Eine Komponente in Netz 1 adressiert eine Komponente in Netz 2 über eine Zieladresse aus dem Adressbereich von Netz 1. Die 1-zu-1-NAT-Funktion bildet die Zieladresse in den Adressbereich von Netz 2 ab. Antworten aus Netz 2 erhalten umgekehrt eine Absenderadresse aus Netz 1.

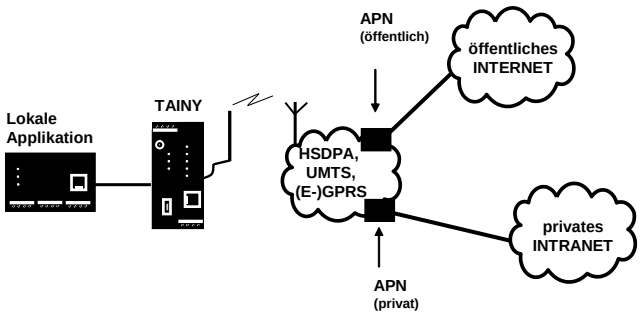
AES

Advanced Encryption Standard.

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit. 1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

APN (Access Point Name)

(Zugriffspunktname). Netzübergreifende Verbindungen, z. B. vom Datenfunkdient (HSDPA, UMTS, EGPRS oder GPRS) ins Internet, werden über sogenannte APNs hergestellt.



Ein Endgerät, das eine Verbindung über den Datenfunkdienst aufbauen will, gibt durch Angabe des APN an, mit welchem Netz es verbunden werden will: Internet oder privates Firmennetz, das über Standleitung angeschlossen ist.

Der APN bezeichnet den Übergabepunkt zum anderen Netz. Er wird dem Benutzer vom Netzbetreiber mitgeteilt.

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.

Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.

Asymmetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwändige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

CIDR

Classless InterDomain Routing

IP-Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinander folgenden Adressen als ein Netzwerk behandelt.

Das CIDR-Verfahren reduziert die z. B. in Routern gespeicherten Routing-Tabellen durch einen Postfix in der IP-Adresse. Mit diesem Postfix können ein Netz und die darunter liegenden Netze zusammengefasst bezeichnet werden. Die Methode ist in RFC 1518 beschrieben.

Um dem TAINY xMOD einen Bereich von IP-Adressen anzugeben z.B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das/der vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.

Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D.h. der Client ist der anrufende Rechner, der Server (oder Host) der Angerufene.

CSD 9600

CSD (9600) steht für Circuit Switched Data oder Daten-Wählverbindung. Dabei wird eine Verbindung zwischen zwei Teilnehmern (Endpunkten der Verbindung) aufgebaut, ähnlich wie bei einem Telefonat im öffentlichen Fernsprechnetz. Teilnehmer 1 wählt die Rufnummer von Teilnehmer 2. Das Netz signalisiert Teilnehmer 2 den Anruf, Teilnehmer 2 nimmt den Ruf an und das Netz baut die Verbindung auf, bis einer der Teilnehmer die Verbindung wieder beendet.

Im GSM-Netz wird dieser Dienst CSD genannt und erlaubt die Datenübertragung mit 9600 bit/s oder 14400 bit/s, wobei die Übertragung gesichert oder ungesichert stattfindet. Möglich sind Verbindungen GSM Modem zu GSM Modem, Analog Modem zu GSM und ISDN-Modem zu GSM-Modem.

CSQ / RSSI

Der CSQ-Wert ist ein im GSM-Standard festgelegter Wert zur Angabe der Signalqualität. CSQ-Werte korrespondieren zur Empfangsfeldstärke RSSI (= Received Signal Strength Indication):

CSQ	***RSSI***
< 6	< -101 dBm
6 - 10	-101 … - 93 dBm
11 – 18	- 91 dBm … -77 dBm
> 18	> 77 dBm
99	Nicht eingebucht

Datagramm

Beim Übertragungsprotokoll TCP/IP werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

1. IP-Header
2. TCP-/UDP-Header
3. Daten (Payload)

Der IP-Header enthält:

- die IP-Adresse des Absenders (source IP-address)
- die IP-Adresse des Empfängers (destination IP-address)
- die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
- die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:

- Port des Absenders (source port)
- Port des Empfängers (destination port)
- eine Prüfsumme über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.

DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.

3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

DHCP

Dynamic Host Configuration Protocol (DHCP) übernimmt die automatische dynamische Zuweisung von IP-Adressen und weiteren Parametern in einem Netzwerk. Das Dynamic Host Configuration Protocol verwendet UDP. Es wurde definiert im RFC 2131 und bekam die UDP-Ports 67 und 68 zugewiesen. DHCP arbeitet im Client – Server Verfahren, wobei der Client vom Server die IP-Adressen zugewiesen bekommt.

DNS

Die Adressierung in IP-Netzen erfolgt grundsätzlich über IP-Adressen. Bevorzugt wird im Allgemeinen aber die Adressierung in Form einer Domain-Adresse angegeben (d. h. in der Form www.abc.xyz.de). Erfolgt die Adressierung über die Domain-Adresse, sendet der Absender zunächst die Domain-Adresse an einen Domain Name Server (DNS) und erhält die dazugehörige IP-Adresse zurück. Erst dann adressiert der Absender seine Daten an diese IP-Adresse.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einen Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.

Soll ein lokaler Rechner über das Internet erreichbar sein, muss seine Adresse der externen Gegenstelle bekannt sein. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat einen Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).

Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.xyz.abc.de. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.

Wenn jetzt ein externer Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der externe Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurück übertragen zum externen Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.

Allen Internetadressen liegt prinzipiell dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz aufgebaut.

EDGE

EDGE (= Enhanced Data Rates for GSM Evolution) bezeichnet eine Technik, bei der die verfügbaren Datenraten in GSM-Mobilfunknetzen durch Einführung eines zusätzlichen Modulationsverfahrens erhöht werden. Mit EDGE werden GPRS zu EGPRS (Enhanced GPRS) und HSCSD zu ECSD erweitert.

EGPRS

EGPRS steht für "Enhanced General Packet Radio Service " und beschreibt einen auf GPRS beruhenden paketorientierten Datendienst, der durch EDGE-Technologie beschleunigt ist.

GPRS

GPRS ist die Abkürzung von "General Packet Radio Service" und ein Datenübertragungssystem von GSM2+ Mobilfunksystemen. GPRS-Systeme nutzen die Basisstationen der GSM-Netze für die Funktechnik und eine eigene Infrastruktur zur Vernetzung und zur Kopplung an andere IP-Netze, wie zum Beispiel dem Internet. Daten werden dabei paket-orientiert vermittelt, wobei das Internet Protokoll (IP) verwendet wird. GPRS stellt Datenraten von bis zu 115,2 KBit/s zur Verfügung.

GSM

GSM (= Global System for Mobile Communication) ist ein weltweit verbreiteter Standard für digitale Mobilfunknetze. GSM unterstützt außer dem Sprachdienst zur Telefonie, verschiedene Datendienste, wie Fax, SMS, CSD und GPRS. Abhängig von gesetzlichen Bestimmungen in den verschiedenen Ländern, werden die Frequenzbänder 900 MHz, 1800 MHz oder 850 MHz und 1900 MHz verwendet.

HSDPA

HSDPA (=High Speed Downlink Packet Access) ist eine Erweiterung des UMTS-Netzes, die höhere Übertragungsraten bei der Datenübertragung von der Basisstation zur Mobilstation ermöglicht.

HTTPS

HTTPS (=HyperText Transfer Protocol Secure) ist eine Variante des bekannten HTTP, wie es von jedem Web-Browser zur Navigation und zum Datenaustausch im Internet verwendet wird. Bekannt ist die Eingabe: http://www.neuhaus.de.

Bei HTTPS ist dem ursprünglichen Protokoll eine zusätzliche Komponente zum Datenschutz hinzugefügt. Während bei HTTP-Daten ungeschützt in Klartext übertragen werden, werden bei HTTPS-Daten erst nach einer Austausch von Sicherheitszertifikaten verschlüsselt übertragen.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.

Eine IP-Adresse besteht aus 2 Teilen: der Netzwerk-Adresse und der Host-Adresse.

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorien Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

	1. Byte	2. Byte	3. Byte	4 Byte
Class A	Netz-Adr.	Host-Adr.		
Class B	Netz-Adr.		Host-Adr.	
Class C	Netz-Adr.			Host-Adr.

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	Bytes für die Netz-Adresse	Bytes für die Host-Adresse
Class A	1-126	1	3
Class B	128-191	2	2
Class C	192-223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

IP-Paket

Siehe Datagramm

IPsec

IP security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPSec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA), der Security-Parameter-Index (SPI) und der Internet Key Exchange (IKE).

Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. Transport Mode oder Tunnel Mode.

Im Transport Mode wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPSec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.

Im Tunnel Mode wird dem gesamten IP-Datagramm ein IPSec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.

Der Tunnel Mode findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrecke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

MIB

Siehe SNMP

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als IP-Masquerading bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über den NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.

Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.

Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den IP- und den TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzten Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.

Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Netzmaske / Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 134.76.0.0. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).

Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu "borgen", um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

Port-Nummer

Das Feld Port-Nummer ist ein 2 Byte großes Feld in UDP- und TCP-Headern. Die Vergabe der Port-Nummern dient der Identifikation der verschiedenen Datenströme, die UDP/TCP gleichzeitig abarbeitet. Über diese Port-Nummern erfolgt der gesamte Datenaustausch zwischen UDP/TCP und den Anwendungsprozessen. Die Vergabe der Port-Nummern an Anwendungsprozesse geschieht dynamisch und wahlfrei. Für bestimmte, häufig benutzte Anwendungsprozesse sind feste Port-Nummern vergeben. Diese werden als Assigned Numbers bezeichnet.

PPPoE

Akronym für Point-to-Point Protocol over Ethernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für Point-to-Point Tunneling Protocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Private Key (privater Schlüssel), Public Key (öffentlicher Schlüssel); Zertifizierung (X.509)

Bei asymmetrischen Verschlüsselungsalgorithmen werden 2 Schlüssel verwendet: ein privater (*Private Key*) und ein öffentlicher (*Public Key*). Der öffentliche Schlüssel dient zum Verschlüsseln von Daten, der private Schlüssel zum Entschlüsseln.

Der öffentliche Schlüssel wird vom zukünftigen Empfänger von Daten denen zur Verfügung gestellt, die die Daten verschlüsselt an ihn versenden werden. Der private Schlüssel ist nur im Besitz des Empfängers. Er dient zum Entschlüsseln der empfangenen Daten.

Zertifizierung:

Damit der Benutzer des (zum Verschlüsseln dienenden) öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung: Die Überprüfung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Absenders mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Absender beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Prüfung signiert die CA den öffentliche Schlüssel des Absenders mit ihrer (digitalen) Unterschrift. Es entsteht ein *Zertifikat*.

Ein X.509-Zertifikat stellt eine Verbindung zwischen einer Identität in Form eines 'X.500 Distinguished Name' (DN) und einem öffentliche Schlüssel her, die durch die digitale Signatur einer X.509 Certification Authority (CA) beglaubigt wird. Die Signatur - eine Verschlüsselung mit dem Signaturschlüssel - kann mit dem öffentlichem Schlüssel überprüft werden, die die CA dem Zertifikatsinhaber aushändigt.

Protokoll, Übertragungs-protokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutzte Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP. TCP/IP ist der Oberbegriff für alle auf IP aufbauenden Protokolle.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Anti-Spoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.

Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

SNMP

SNMP (Simple Network Management Protokoll) ist ein weitverbreiteter Mechanismus zur zentralen Kontrolle und Steuerung von Netzwerk-Komponenten wie zum Beispiel Server, Router, Switches, Drucker, Computer usw..

SNMP definiert den Kommunikationsablauf und den Aufbau der Datenpakete. Zum Transport wird UDP über IP verwendet.

SNMP definiert nicht die Werte, die gelesen oder verändert werden können.

Dies geschieht in einer MIB (Management Information Base). Die MIB ist eine Beschreibungsdatei, in denen die einzelnen Werte tabellarisch aufgeführt werden. Die MIB ist jeweils spezifisch für eine bestimmte Netzwerkkomponente oder für eine Klasse von Komponenten, zum Beispiel Switches.

SNMP-Trap

SNMP-Trap ist eine Benachrichtigung die mittels SNMP Agent (Simple Network Management Protokoll) von einer Netzwerk-Komponente unaufgefordert versendet wird.

SSH

SSH (Secure SHell) ist ein Protokoll, das den gesicherten und verschlüsselten Datenaustausch zwischen Rechnern ermöglicht. Verwendet wird Secure SHell zum Fernzugriff auf die Eingabekonsole von LINUX-basierten Maschinen.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/Internet Protocol

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.

IP ist das Basisprotokoll.

UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.

TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.

UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.

Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).

ICMP baut auf IP auf und enthält Kontrollnachrichten.

SMTP ist ein auf TCP basierendes E-Mail-Protokoll.

IKE ist ein auf UDP basierendes IPsec-Protokoll.

ESP ist ein auf IP basierendes IPsec-Protokoll.

Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.

(→ Datagramm)

UDP

Siehe TCP/IP

UMTS

UMTS (Universal Mobile Telecommunication System) ist ein Mobilfunknetz der 3. Generation, das deutlich höhere Datenübertragungsraten ermöglicht, als die GSM-Netze der 2. Generation. UMTS bietet neben der Sprachübertragung, IP-basierte Datenübertragung und SMS-Übertragung auch die Möglichkeit zu Übertragung von Videoanwendungen.

Mit Ausnahme des nordamerikanisches Raums verwendet UMTS ein Frequenzband bei 2100 MHz. In Nordamerika werden die Frequenzbänder bei 850 MHz und 1900 MHz genutzt, die auch für GSM-Netze verwendet werden.

VPN (Virtuelles Privates Netzwerk)

Ein Virtuelles Privates Netzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

X.509-Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (Certification Authority - CA). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3)-Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguished Name (DN)), erlaubte Verwendungszwecke usw. und der Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

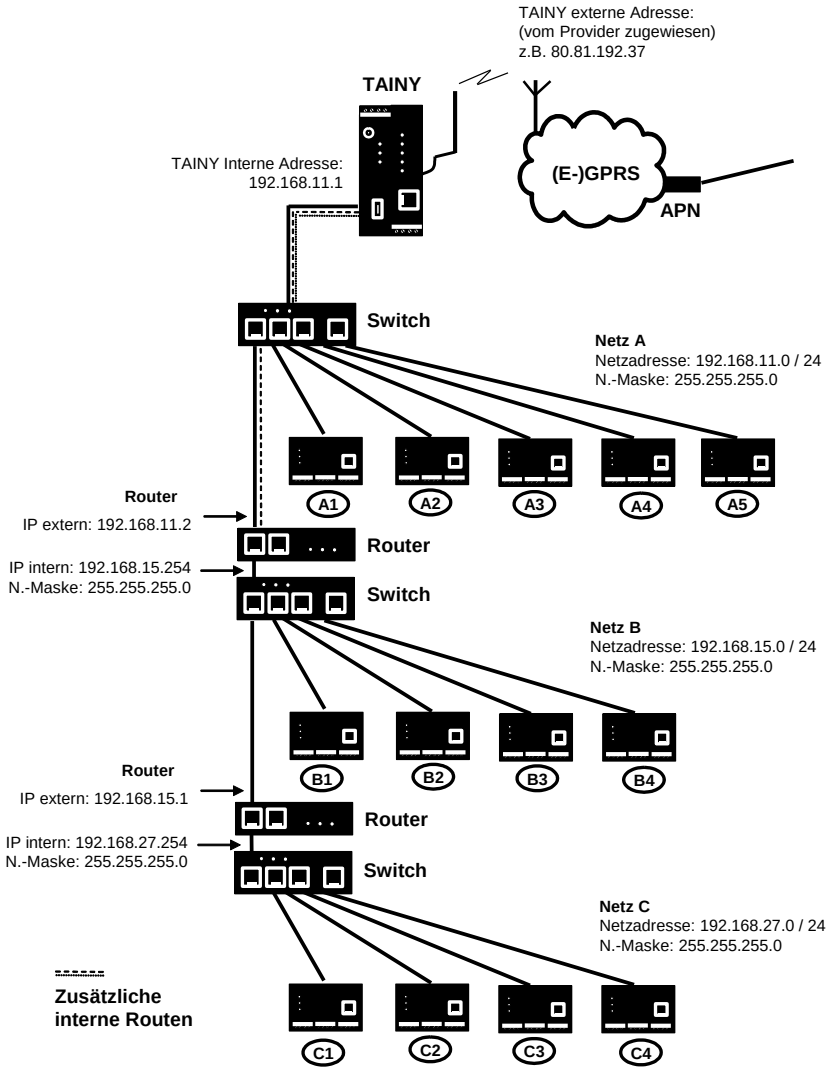
Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509-Zertifikate kommen z.B. bei E-Mail-Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Zusätzliche interne Routen

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A ist an das TAINY xMOD angeschlossen und über dieses mit einem entfernten Netz verbunden. Zusätzliche interne Routen zeigen den Weg zu weiteren Netzen (Netz B, C), die über Gateways (Router) miteinander verbunden sind. Für das TAINY xMOD sind bei dem gezeigten Beispiel die Netze B und C beide über das Gateway 192.168.11.2 und die Netzwerkadresse 192.168.11.0/24 erreichbar.

Netz A					
Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Netz B					
Rechner	B1	B2	B3	B4	**Zusätzliche interne Routen:**
IP-Adresse	192.168.15.3	192.168.15.4	192.168.15.5	192.168.15.6	Netzwerk: 192.168.15.0/24 Gateway: 192.168.11.2
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
Netz C					Netzwerk: 192.168.27.0/24 Gateway: 192.168.11.2
Rechner	C1	C2	C3	C4	
IP-Adresse	192.168.27.3	192.168.27.4	192.168.27.5	192.168.27.6	
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	

13 Technische Daten

13.1 TAINY HMOD-V2-IO, TAINY HMOD-L1-IO

Schnittstellen	Applikations-Schnittstelle	10/100 Base-T (RJ45 plug) Ethernet IEEE802 10/100 Mbit/s
	Service Schnittstelle	USB-A (reserviert für spätere Anwendungen)
Sicherheits-Funktionen	VPN	IPSec (nur TAINY HMOD-V2-IO) Etwa 10 VPN-Tunnel
	Firewall	Stateful Inspection Firewall Anti-Spoofing Port Weiterleitung
Weitere Funktionen		DNS Cache, DHCP-Server, NTP, Remote Logging, Verbindungsüberwachung, Alarm-SMS
Management		Web-basierte Administrations-Oberfläche,ssh-Konsole
Funkverbindung	Frequenzbänder	UMTS/HSDPA: Triple band, 850//1900/2100MHz GSM/GPRS/EDGE: Quad band, 850/900/1800/1900MHz
	HSDPA UMTS	3.6 Mbps, UL 384 kbps UE CAT. [1-6], 11, 12 supported Compressed mode (CM) supported according to 3GPP TS25.212 PS data rate – 384 kbps DL / 384 kbps UL CS data rate – 64 kbps DL / 64 kbps UL
	EDGE (EGPRS)	EDGE Multislot class 12 / EDGE Multislot class 12 Multislot Class 10 Mobile Station Class B PBCCH support Downlink coding schemes – CS 1-4, MCS 1-9 Uplink coding schemes – CS 1-4, MCS 1-9
	GPRS	Multislot Class 10 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	CSD / MTC	V.110, RLP, non-transparent 9.6 kbps
	SMS (TX)	Punkt zu Punkt, MO (abgehend)
	Antennen-anschluss	Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperatur-bereich	Betrieb: -20 °C bis +60 °C Lagerung: -40 °C bis +70 °C
	Luftfeuchte	0-95 %, nicht kondensierend

Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff
	Schutzklasse	IP20
	Abmessungen	114 mm x 45 mm x 99 mm
	Gewicht	ca. 280g
Konformität	CE	Ja
	R&TTE (GSM)	Konform zur Richtlinie 99/05/EC Angewandte Norm: EN301 511 v.9.0.2, EN301 908-1/-2: v.4.2.1
	HSDPA/UMTS/ GSM/EGPRS-Modul	Konform zu GCF, PTCRB
	EMV/ESD	Angewandte Normen: EN 55022:2010 Klasse A, EN 55024: 1998 + A1:2001 + A2:2003, EN 61000-6-2:2005
	Elektrische Sicherheit	Angewandte Norm: EN 60950:2006 + A11:2009 + A1:2010
	Umwelt	Das Gerät entspricht den europäischen Richtlinien ROHS und WEEE.
Spannungsversorgung	Eingangs-spannung	12 - 60 V DC (24 V DC nominal)
	Leistungs-aufnahme	Typisch 4,4 W bei 12 V Typisch 4,0 W bei 24 V Typisch 5,5 W bei 60 V
	Stromaufnahme	450mA bei 12V und 100mA bei 60V Iburst = 1,26A

13.2 TAINY EMOD-V2-IO, TAINY EMOD-L1-IO

Schnittstellen	Applikations-Schnittstelle	10/100 Base-T (RJ45 plug) Ethernet IEEE802 10/100 Mbit/s
	Service Schnittstelle	USB-A (reserviert für spätere Anwendungen)
Sicherheits-Funktionen	VPN	IPSec (nur TAINY EMOD-V2-IO)
	Firewall	Stateful Inspection Firewall Anti-Spoofing Port Weiterleitung
Weitere Funktionen		DNS Cache, DHCP-Server, NTP, Remote Logging, Verbindungsüberwachung, Alarm-SMS
Management		Web-basierte Administrations-Oberfläche,ssh-Konsole
Funkverbindung	EDGE / GPRS	EDGE Multislot class 12 / EDGE Multislot class 12
	Coding schemes GSM Module	CS-1, CS-2, CS-3, CS-4 EGPRS (EDGE) / Quad band
	EDGE (EGPRS)	Multislot Class 12 Mobile Station Class B Modulation and Coding Scheme MCS 1 – 9
	GPRS	Multislot Class 12 Full PBCCH support Mobile Station Class B Coding Scheme 1 – 4
	EDGE / GPRS	Während der Datenübertragung über EGPRS oder GPRS wählt das Gerät automatisch zwischen folgenden Klassen aus: - von EGPRS Multislot Class 12 (4Tx slots) bis EGPRS Multislot Class 10 (2Tx slots), - von EGPRS Multislot Class 10 (2Tx slots) bis EGPRS Multislot Class 8 (1Tx), - von GPRS Multislot Class 12 (4Tx slots) bis GPRS Multislot Class 8 (1Tx) - von GPRS Multislot Class 10 (2Tx slots) bis GPRS Multislot Class 8 (1Tx)
	CSD / MTC	V.110, RLP, non-transparent 2.4, 4.8, 9.6, 14.4kbps
	SMS (TX)	Punkt zu Punkt, MO (abgehend)

	Max. Sendeleistung (gemäß Ausgabe 99, V5)	Class 4 (+33dBm ±2dB) for EGSM850 Class 4 (+33dBm ±2dB) for EGSM900 Class 1 (+30dBm ±2dB) for GSM1800 Class 1 (+30dBm ±2dB) for GSM1900 Class E2 (+27dBm ± 3dB) for GSM 850 8-PSK Class E2 (+27dBm ± 3dB) for GSM 900 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1800 8-PSK Class E2 (+26dBm +3 /-4dB) for GSM 1900 8-PSK
	Antennen-anschluss	Impedanz nominal: 50 Ohm, Buchse: SMA
Umwelt-bedingungen	Temperatur-bereich	Betrieb: -20 °C bis +60 °C Lagerung: -40 °C bis +70 °C
	Luftfeuchte	0-95 %, nicht kondensierend
Gehäuse	Ausführung	Hutschienengehäuse
	Material	Kunststoff
	Schutzklasse	IP20
	Abmessungen	114 mm x 45 mm x 99 mm
	Gewicht	ca. 280g
Konformität	CE	Ja
	R&TTE (GSM)	Konform zur Richtlinie 99/05/EC Angewandte Norm: EN301 511 v.9.0.2
	GSM/EGPRS-Modul	Konform zu GCF, PTCRB
	EMV/ESD	Angewandte Normen: EN 55022:2010 Klasse A, EN 55024: 1998 + A1:2001 + A2:2003, EN 61000-6-2:2005
	Elektrische Sicherheit	Angewandte Norm: EN 60950:2006 + A11:2009 + A1:2010
	Umwelt	Das Gerät entspricht den europäischen Richtlinien ROHS und WEEE.
Spannungsversorgung	Eingangs-spannung	12 - 60 V DC (24 V DC nominal)
	Leistungs-aufnahme	Typisch 4,4 W bei 12 V Typisch 4,0 W bei 24 V Typisch 5,5 W bei 60 V
	Stromaufnahme	450mA bei 12V und 100mA bei 60V Iburst = 1,26A